

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE COUNTY OF ORANGE SOCIAL SERVICES AGENCY
AND
MAXIMUS, INC.
FOR THE PROVISION OF
HEALTH CARE OPTIONS

This Memorandum of Understanding (MOU) is entered into by and between the County of Orange, acting through its Social Services Agency (SSA), hereinafter referred to as “COUNTY,” and Maximus, Inc., hereinafter referred to as “MAXIMUS.” This MOU establishes the procedures to allow MAXIMUS to provide health plan enrollment and education services for the Medi-Cal managed care plans (MCP) for Medi-Cal applicants and beneficiaries.

COUNTY and MAXIMUS may be referred to individually as “Party” and collectively as “the Parties.” The relationship between COUNTY and MAXIMUS, with regard to this MOU, is based upon the following:

1. This MOU is authorized and provided for pursuant to Welfare and Institutions Code (WIC) section 14197.11, and WIC sections 14094.4, 14094.5, 14094.6, 14016.5(a), and 14016.6, and All County Welfare Directors Letter (ACWDL) No. 12-28.
2. This MOU sets forth the procedures authorized by both the COUNTY’s SSA Director and MAXIMUS, for their respective employees to follow in providing services under this MOU.
3. This non-financial MOU is a legally binding agreement based on the promises of the Parties.

TABLE OF CONTENTS

1. TERM 3

2. PURPOSE 3

3. POPULATION TO BE SERVED 3

4. MAXIMUS RESPONSIBILITIES 3

5. COUNTY RESPONSIBILITIES..... 4

6. FACILITIES..... 4

7. USE OF COUNTY PROPERTY 5

8. NON-DISCRIMINATION..... 6

9. CONFIDENTIALITY 9

10. PUBLICITY, LITERATURE, ADVERTISEMENTS AND SOCIAL MEDIA..... 10

11. INDEMNIFICATION..... 11

12. INSURANCE 12

13. SECURITY 17

14. NOTIFICATION OF INCIDENTS, CLAIMS, OR SUITS..... 17

15. RECORDS 17

16. PERSONNEL DISCLOSURE 18

17. CHILD AND DEPENDENT ADULT/ELDER ABUSE REPORTING 20

18. NOTICE TO EMPLOYEES REGARDING THE SAFELY SURRENDERED BABY
LAW 21

19. NOTICES..... 21

20. RESOLUTION OF CONFLICTS 22

21. CONFLICT OF INTEREST 22

22. POLITICAL ACTIVITY 22

23. TERMINATION 22

24. SIGNATURE IN COUNTERPARTS 24

25. GENERAL PROVISIONS..... 24

ATTACHMENTS

Attachment A – SSA Policy and Procedure I 6: Information Technology Security and Usage

Attachment B – SSA Policy and Procedure F 21: Privacy and Security Incidents of Personally Identifiable Information (PII) and Confidential Information

Attachment C – County of Orange Information Technology Security Provisions

Attachment D – State Privacy and Security Provisions

Attachment E – License Agreements

Attachment F – Agreement number 17-94437 between the State of California Department of Health Care Services (DHCS) and MAXIMUS

1. TERM

The term of this MOU shall commence on January 1, 2024, and end on June 30, 2027, unless earlier terminated pursuant to the provisions of Paragraph 23 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, reporting, and confidentiality.

2. PURPOSE

The purpose of this MOU is to define the roles and responsibilities surrounding MAXIMUS' provision of Health Care Options (HCO) services for COUNTY'S Medi-Cal applicants and beneficiaries pursuant to WIC sections 14197.11, 14094.4, 14094.5, 14094.6, 14016.5(a), and 14016.6, and ACWDL No. 12-28.

3. POPULATION TO BE SERVED

3.1 MAXIMUS shall provide HCO services to Medi-Cal applicants and beneficiaries referred by SSA that meet certain criteria for Medi-Cal managed care plan enrollment. The population to be served as defined in this Paragraph shall hereinafter be referred to as "MEMBERS."

4. MAXIMUS RESPONSIBILITIES

4.1 Provide health plan enrollment and education services in the County of Orange pursuant to Agreement number 17-94437 between the State of California Department of Health Care Services (DHCS) and MAXIMUS attached as Attachment F to this MOU;

4.2 Provide health care services through networks of organized systems of care;

4.3 Ensure access to health care through an enrollment broker contractor which gives information to MEMBERS about managed care plans;

4.4 Assist MEMBERS to make informed choices about their Medi-Cal benefits;

4.5 Provide staffing subject to DHCS agreed upon full-time equivalent (FTE) allocations;

- 4.6 Provide services during hours that are responsive to the needs of the target population(s) as determined by COUNTY. At a minimum, MAXIMUS shall provide services Monday through Friday, from 8:00 a.m. to 5:30 p.m., except COUNTY holidays as established by the Orange County Board of Supervisors;
 - 4.7 Provide trained, culturally, and linguistically capable Enrollment Services Representatives to conduct scheduled HCO presentations under a mutually agreed upon published schedule;
 - 4.8 Provide bilingual staff to serve MEMBERS who speak English, and Spanish. All other language requirements will be supported through the assistance of the Health Care Options (HCO) Call Center, which offers remote language support to Enrollment Services Representatives statewide;
 - 4.9 At MAXIMUS' expense, utilize outside translation services for MEMBERS whose primary language is other than those listed in Subparagraph 4.8 above or any other language in which MAXIMUS staff are not fluent;
 - 4.10 Develop and implement an HCO referral document which shall be subject to modification upon mutual agreement of the Parties to meet COUNTY needs; and
 - 4.11 Provide necessary training for all designated MAXIMUS staff on HCO services for MEMBERS pursuant to agreement number 17-94437 as referenced above in subparagraph 4.1.
5. COUNTY RESPONSIBILITIES
- 5.1 Assist MEMBERS by answering questions about the MCP Transition health plan changes and supporting transition of their Medi-Cal MCP;
 - 5.2 Differentiate the MCP Transition from MEMBER eligibility redetermination;
 - 5.3 Direct MEMBERS to DHCS Transition webpages; and
 - 5.4 Direct MEMBERS to MAXIMUS for information about health plan and provider options.
6. FACILITIES

- 6.1 It is mutually understood that MAXIMUS will provide services at the following facilities:

Anaheim Regional Center
3320 E. La Palma Ave.
Anaheim, CA 92806

Garden Grove Regional Center
12912 Brookhurst St.
Garden Grove, CA 92840

Laguna Hills Regional Center
23330 Moulton Pkwy
Laguna Hills, CA 92653

Santa Ana Regional Center
1928 S. Grand Ave.
Santa Ana, CA 92705

- 6.2 MAXIMUS and COUNTY may mutually agree in writing to add, change, modify, or delete facility location(s) as necessary to best serve the needs of COUNTY and clients to be served under this MOU.

7. USE OF COUNTY PROPERTY

- 7.1 MAXIMUS shall be co-located with COUNTY staff, at a COUNTY facility, to provide services under this MOU. MAXIMUS shall enter into a rent-free license agreement with COUNTY for the co-location and shall execute all terms and conditions of said agreement upon COUNTY's presentation of said document to MAXIMUS. Failure to execute and abide by the license agreement will result in

a breach of this MOU.

7.2 MAXIMUS is responsible for any costs associated with Fair Employment and Housing Act and Americans with Disabilities Act accommodations for its own employees at COUNTY facilities. COUNTY, may, at its sole discretion and on a case-by-case basis, provide for such accommodations at no cost to MAXIMUS.

7.3 Use of COUNTY Computer Equipment

COUNTY may permit MAXIMUS the use of computer equipment provided by COUNTY. Said computer equipment shall be used solely by employees of MAXIMUS while performing their assigned duties pursuant to this MOU and shall remain the property of COUNTY. MAXIMUS shall ensure that each of its employees, volunteers, consultants, or agents that have access to COUNTY facilities and/or data contained in COUNTY's Computer Information System completes information security and computer usage training provided by COUNTY, and adheres to the provisions in Attachments A, B, C, and D, to this MOU, signs and adheres to the provisions in SSA Information Technology Security and Usage Agreement as referenced and included in Attachment A, and adheres to any subsequent contracts required by federal or State laws or regulations. MAXIMUS's failure to have all MAXIMUS employees that have access to COUNTY's facilities and/or data execute the agreements and/or complete the training shall constitute a breach of this MOU.

8. NON-DISCRIMINATION

8.1 In the performance of this MOU, MAXIMUS agrees that it shall not engage nor employ any unlawful discriminatory practices in the admission of clients, provision of services or benefits, assignment of accommodations, treatment, evaluation, employment of personnel, or in any other respect, on the basis of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender,

gender identity, gender expression, age, sexual orientation, military and veteran status, or any other protected group, in accordance with the requirements of all applicable federal or State laws.

8.2 MAXIMUS shall furnish any and all information requested by COUNTY and shall permit COUNTY access, during business hours, to books, records, and accounts in order to ascertain MAXIMUS's compliance with Paragraph 8 et seq.

8.3 Non-Discrimination in Employment

8.3.1 All solicitations or advertisements for employees placed by or on behalf of MAXIMUS shall state that all qualified applicants will receive consideration for employment without regard to race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, military and veteran status, or any other protected group, in accordance with the requirements of all applicable federal or State laws. Notices describing the provisions of the equal opportunity clause shall be posted in a conspicuous place for employees and job applicants.

8.3.2 MAXIMUS shall refer any and all employees desirous of filing a formal discrimination complaint to:

California Department of Fair Employment

2218 Kausen Drive, Suite 100

Elk Grove, CA 95758

Telephone: (800) 884-1684

(800) 700-2320 (TTY)

8.4 Non-Discrimination in Service Delivery

8.4.1 MAXIMUS shall comply with Titles VI and VII of the Civil Rights Act of 1964, as amended; Section 504 of the Rehabilitation Act of 1973, as

amended; the Age Discrimination Act of 1975, as amended; the Food Stamp Act of 1977, as amended, and in particular 7 Code of Federal Regulations (CFR) section 272.6; Title II of the Americans with Disabilities Act of 1990; California Civil Code Section 51 et seq., as amended; California Government Code (CGC) Sections 11135-11139.5, as amended; CGC Section 12940 (c), (h), (i), and (j); CGC Section 4450; Title 22, California Code of Regulations (CCR) Sections 98000-98413; the Dymally-Alatorre Bilingual Services Act (CGC Section 7290-7299.8); Section 1808 of the Removal of Barriers to Interethnic Adoption Act of 1996; and other applicable federal and State laws, as well as their implementing regulations (including Title 45 CFR Parts 80, 84, and 91; Title 7 CFR Part 15; and Title 28 CFR Part 42), and any other law pertaining to Equal Employment Opportunity, Affirmative Action, and Nondiscrimination, as each may now exist or be hereafter amended. MAXIMUS shall not implement any administrative methods or procedures which would have a discriminatory effect or which would violate the California Department of Social Services (CDSS), Manual of Policies and Procedures (MPP) Division 21, Chapter 21-100. If there are any violations of this Paragraph, CDSS shall have the right to invoke fiscal sanctions or other legal remedies in accordance with California Welfare and Institutions Code (WIC) Section 10605, or CGC Sections 11135-11139.5, or any other laws, or the issue may be referred to the appropriate federal agency for further compliance action and enforcement of Subparagraph 8 et seq.

8.4.2 MAXIMUS shall provide any and all clients desirous of filing a formal complaint any and all information as appropriate:

8.4.2.1 Pamphlet: “Your Rights Under California Welfare Programs”

(PUB 13)

8.4.2.2 Discrimination Complaint Form

8.4.2.3 Civil Rights Contacts

County Civil Rights Contact

Orange County Social Services Agency

Program Integrity

Attn: Civil Rights Coordinator

P.O. Box 22001

Santa Ana, CA 92702-2001

Telephone: (714) 438-8877

State Civil Rights Contact

California Department of Social Services

Civil Rights Bureau

P.O. Box 944243, M/S 8-16-70

Sacramento, CA 94244-2430

Federal Civil Rights Contact

Office for Civil Rights

U.S. Department of Health and Human Services

90 7th Street, Suite 4-100

San Francisco, CA 94103

Customer Response Center: (800) 368-1019

9. CONFIDENTIALITY

9.1 COUNTY and MAXIMUS agree to maintain confidentiality of all records pursuant to WIC Sections 827 and 10850-10853, 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.

- 9.2 All records and information concerning any and all persons referred to MAXIMUS by COUNTY or COUNTY's designee shall be considered and kept confidential by MAXIMUS, MAXIMUS's employees, agents, and all other individuals performing services under this MOU. MAXIMUS shall require all of its employees, agents, and all other individuals performing services under this MOU to sign an agreement with MAXIMUS before commencing the provision of any such services, agreeing to maintain confidentiality pursuant to this MOU.
- 9.3 MAXIMUS shall inform all of its employees, agents, and all other individuals performing services under this MOU of this provision and that any person violating the provisions of said California state law may be guilty of a crime.
- 9.4 MAXIMUS agrees to maintain the confidentiality of its records with respect to Juvenile Court matters, in accordance with WIC Section 827, all applicable statutes, case law, and Orange County Juvenile Court Policy regarding Confidentiality, as it now exists or may hereafter be amended.
- 9.4.1 No access, disclosure, or release of information regarding a child who is the subject of Juvenile Court proceedings shall be permitted except as authorized. If authorization is in doubt, no such information shall be released without the written approval of a Judge of the Juvenile Court.
- 9.4.2 MAXIMUS must receive prior written approval of the Juvenile Court before allowing any child to be interviewed, photographed, or recorded by any publication or organization, or to appear on any radio, television, or internet broadcast or make any other public appearance. Such approval shall be requested through child's Social Worker.
10. PUBLICITY, LITERATURE, ADVERTISEMENTS AND SOCIAL MEDIA
- 10.1 COUNTY owns all rights to the name, logos, and symbols of COUNTY. The use and/or reproduction of COUNTY's name, logos, or symbols for any purpose, including commercial advertisement, promotional purposes, announcements,

displays, or press releases, without COUNTY's prior written consent is expressly prohibited.

10.2 MAXIMUS may develop and publish information related to this MOU where all of the following conditions are satisfied:

10.2.1 COUNTY provides its written approval of the content and publication of the information at least 30 days prior to MAXIMUS publishing the information, unless a different timeframe for approval is agreed upon by COUNTY;

10.2.2 Unless directed otherwise by COUNTY, the information includes a statement that the program, wholly or in part, is funded through County, State, and Federal Government funds;

10.2.3 The information does not give the appearance that the COUNTY, its officers, employees, or agencies endorse:

10.2.3.1 any commercial product or service; and

10.2.3.2 any product or service provided by MAXIMUS, unless approved in writing by COUNTY;

10.2.4 If MAXIMUS uses social media (such as Facebook, Twitter, YouTube, or other publicly available social media sites) to publish information related to this MOU, MAXIMUS shall develop social media policies and procedures and have them available to the COUNTY. MAXIMUS shall comply with COUNTY Social Media Use Policy and Procedures as they pertain to any social media developed in support of the services described within this MOU. The policy is available on the Internet at <https://cio.ocgov.com/egovernment-policies>.

11. INDEMNIFICATION

11.1 MAXIMUS 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 MAXIMUS pursuant to this MOU. If judgment is entered against MAXIMUS and COUNTY by a court of competent jurisdiction because of the concurrent active negligence of COUNTY or COUNTY INDEMNITEES, MAXIMUS and COUNTY agree that liability will be apportioned as determined by the court. Neither Party shall request a jury apportionment.

12. INSURANCE

- 12.1 Prior to the provision of services under this MOU, MAXIMUS agrees to carry all required insurance at MAXIMUS's expense, including all endorsements required herein, necessary to satisfy COUNTY that the insurance provisions of this MOU have been complied with. MAXIMUS agrees to keep such insurance coverage current, provide Certificates of Insurance and endorsements to COUNTY during the entire term of this MOU.
- 12.2 All self-insured retentions (SIRs) shall be clearly stated on the Certificate of Insurance. Any SIRs in excess of fifty thousand dollars (\$50,000), shall specifically be approved by the County's Risk Manager, or designee. COUNTY reserves the right to require current audited financial reports from MAXIMUS. If MAXIMUS is self-insured, MAXIMUS will indemnify COUNTY for any and all claims resulting or arising from MAXIMUS's services in accordance with the indemnity provision stated in this MOU.
- 12.3 If MAXIMUS fails to maintain insurance acceptable to COUNTY for the full term of this MOU, COUNTY may terminate this MOU.

12.4 Qualified Insurer:

12.4.1 The policy or policies of insurance 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).

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

12.4.3 The policy or policies of insurance maintained by MAXIMUS 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
Automobile Liability including coverage for owned or scheduled, non-owned, and hired vehicles	\$2,000,000 aggregate \$1,000,000 combined single limit each accident
Workers' Compensation	Statutory
Employer's Liability Insurance	\$1,000,000 per accident or disease
Network Security & Privacy Liability	\$1,000,000 per claims-made
Sexual Misconduct Liability	\$1,000,000 per occurrence

12.4.4 Increased insurance limits may be satisfied with Excess/Umbrella policies. Excess/Umbrella policies when required must provide Follow

Form coverage.

12.5 Required Coverage Forms

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

12.5.2 Business Auto Liability coverage shall be written on ISO form CA 00 01, CA 00 05, CA 0012, CA 00 20, or a substitute form providing coverage at least as broad.

12.6 Required Endorsements

12.6.1 Commercial General Liability policy shall contain the following endorsements, which shall accompany the Certificate of Insurance:

12.6.1.1 An Additional Insured endorsement using ISO form CG 20 26 04 13, or a form at least as broad, naming the County of Orange, its elected and appointed officials, officers, employees, and agents as Additional Insureds, or provide blanket coverage, which will state AS REQUIRED BY WRITTEN CONTRACT.

12.6.1.2 A primary non-contributory endorsement using ISO form CG 20 01 04 13, or a form at least as broad, evidencing that MAXIMUS' insurance is primary and any insurance or self-insurance maintained by the County shall be excess and non-contributory.

12.6.2 The Workers' Compensation policy shall contain a waiver of subrogation endorsement waiving all rights of subrogation against the County of Orange, its elected and appointed officials, officers, employees, and agents or provide blanket coverage, which will state AS REQUIRED BY WRITTEN CONTRACT.

12.6.3 The Network Security and Privacy Liability policy shall contain the

following endorsements which shall accompany the Certificate of Insurance.

12.6.3.1 An Additional Insured endorsement naming the County of Orange, its elected and appointed officials, officers, employees, and agents as Additional Insureds for its vicarious liability.

12.6.3.2 A primary and non-contributory endorsement evidencing that MAXIMUS's insurance is primary and any insurance or self-insurance maintained by the County shall be excess and non-contributing.

12.7 All insurance policies required by this MOU shall waive all rights of subrogation against the County of Orange, its elected and appointed officials, officers, employees, and agents when acting within the scope of their appointment or employment.

12.8 MAXIMUS shall provide thirty (30) days prior written notice to COUNTY of any policy cancellation or non-renewal and ten (10) days prior written notice where cancellation is due to non-payment of premium and provide a copy of the cancellation notice to COUNTY. Failure to provide written notice of cancellation may constitute a material breach of the contract, upon which the COUNTY may suspend or terminate this MOU.

12.9 If MAXIMUS's Network Security & Privacy Liability policy is a "Claims-Made" policy, MAXIMUS shall agree to the following:

12.9.1 The retroactive date must be before the date of the Contract or the beginning of the Contract services.

12.9.2 Insurance must be maintained, and evidence of insurance must be provided for at least three (3) years after expiration or earlier termination of Contract services.

- 12.9.3 If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the effective date of the Contract services, Contractor must purchase an extended reporting period for a minimum of three (3) years after expiration of or earlier termination of the Contract.
- 12.10 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).
- 12.11 Insurance certificates should be forwarded to COUNTY at the address indicated in Paragraph 19 of this MOU.
- 12.12 Failure of MAXIMUS to provide the insurance certificates and endorsements within seven (7) days of notification by CEO/County Procurement Office or COUNTY, will result in a breach of this MOU.
- 12.13 COUNTY expressly retains the right to require MAXIMUS 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.
- 12.14 COUNTY shall notify MAXIMUS in writing of changes in the insurance requirements. If MAXIMUS does not provide acceptable Certificates of Insurance and endorsements to COUNTY incorporating such changes within thirty (30) days of receipt of such notice, this MOU may be in breach without further notice to MAXIMUS, and COUNTY shall be entitled to all legal remedies.
- 12.15 The procuring of such required policy or policies of insurance shall not be construed to limit MAXIMUS’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.

13. SECURITY

MAXIMUS shall abide by the requirements in Attachments A and C.

14. NOTIFICATION OF INCIDENTS, CLAIMS, OR SUITS

MAXIMUS shall report to COUNTY, in writing within twenty-four (24) hours of occurrence, the following:

14.1 Any accident or incident relating to services performed under this MOU that involves injury or property damage which may result in the filing of a claim or lawsuit against MAXIMUS and/or COUNTY.

14.2 Any third party claim or lawsuit filed against MAXIMUS arising from or relating to services performed by MAXIMUS under this MOU.

14.3 Any injury to an employee of MAXIMUS that occurs on COUNTY property.

14.4 Any loss, disappearance, destruction, misuse, or theft of any kind whatsoever of COUNTY property, monies, or securities entrusted to MAXIMUS under the term of this MOU.

15. RECORDS

15.1 Client Records

15.1.1 MAXIMUS shall prepare and maintain accurate and complete records of clients served and dates and type of services provided under the terms of this MOU in a form acceptable to COUNTY.

15.1.2 MAXIMUS shall keep all COUNTY data provided to MAXIMUS during the term(s) of this for a minimum of five (5) years from the date of final payment under this MOU or until all pending COUNTY, State, and federal audits are completed, whichever is later. These records shall be stored in Orange County, unless MAXIMUS requests and COUNTY provides written approval for the right to store the records in another county. Notwithstanding anything to the contrary, upon termination of this MOU, MAXIMUS shall relinquish control with respect to COUNTY

data to COUNTY in accordance with Subparagraph 23.3 of this contract.

15.2 Public Records

To the extent permissible under the law, 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.

16. PERSONNEL DISCLOSURE

16.1 This Paragraph 16 applies to all of MAXIMUS's personnel providing services through this MOU, paid and unpaid (herein referred to as "Personnel").

16.2 MAXIMUS shall make available to COUNTY a current list of all Personnel providing services hereunder, including résumés and job applications. Changes to the list will be immediately provided to COUNTY in writing, along with a copy of a résumé and/or job application. The list shall include:

16.2.1 Names and dates of birth of all Personnel by title, whose direct services are required to provide the programs described herein;

16.2.2 A brief description of the functions of each position and the hours each person works each week, or for part-time Personnel, each day or month, as appropriate;

16.2.3 The professional degree, if applicable, and experience required for each position; and

16.2.4 The language skill, if applicable, for all Personnel.

16.3 Where authorized by law, and in a manner consistent with California Government Code §12952, MAXIMUS shall require prospective Personnel to provide detailed information regarding the conviction of a crime, by any court, for offenses other than minor traffic offenses. Information discovered subsequent to the hiring or promotion of any prospective Personnel shall be cause for termination from the performance of services under this MOU.

- 16.4 Where authorized by law, MAXIMUS shall conduct, at no cost to COUNTY, a clearance on the following public websites of the names and dates of birth for all Personnel who will have direct, interactive contact with clients served through this MOU: U.S. Department of Justice National Sex Offender Website (www.nsopw.gov) and Megan's Law Sex Offender Registry (www.meganslaw.ca.gov).
- 16.5 Where authorized by law, MAXIMUS shall conduct, at no cost to COUNTY, a criminal record background check on all Personnel who will have direct, interactive contact with clients served through this MOU. Background checks conducted through the California Department of Justice shall include a check of the California Central Child Abuse Index, when applicable. Candidates will satisfy background checks consistent with this Paragraph and their performance of services under this MOU.
- 16.6 MAXIMUS shall ensure that clearances and background checks described in Subparagraphs 16.4 and 16.5 are completed prior to CONTRACTOR's Personnel providing services under this MOU.
- 16.7 In the event a record is revealed through the processes described in Subparagraphs 16.4 and 16.5, COUNTY will be available to consult with MAXIMUS on appropriateness of Personnel providing services through this MOU.
- 16.8 MAXIMUS warrants that all Personnel assigned by MAXIMUS to provide services under this MOU have satisfactory past work records and/or reference checks indicating their ability to perform the required duties and accept the kind of responsibility anticipated under this MOU. MAXIMUS shall maintain records of background investigations and reference checks undertaken and coordinated by MAXIMUS for Personnel assigned to provide services under this MOU, for a minimum of five (5) years from the date of final payment under this MOU, or until all pending COUNTY, State, and federal audits are completed, whichever is

later, in compliance with all applicable laws.

- 16.9 MAXIMUS shall immediately notify COUNTY concerning the arrest and/or subsequent conviction, for offenses, other than minor traffic offenses, of any Personnel performing services under this MOU, when such information becomes known to MAXIMUS. COUNTY, at its sole discretion, may determine whether such Personnel may continue to provide services under this MOU and shall provide notice of such determination to MAXIMUS in writing. MAXIMUS's failure to comply with COUNTY's decision shall be deemed a material breach of this MOU.
- 16.10 COUNTY has the right to approve or disapprove all of MAXIMUS's Personnel performing work hereunder, and any proposed changes in MAXIMUS's Personnel.
- 16.11 COUNTY shall have the right to require MAXIMUS to remove any Personnel from the performance of services under this MOU. At the request of COUNTY, MAXIMUS shall immediately replace said Personnel.
- 16.12 MAXIMUS shall notify COUNTY immediately when Personnel is terminated for cause from working on this MOU.
- 16.13 Disqualification, if any, of MAXIMUS Personnel, pursuant to this Paragraph 16, shall not relieve MAXIMUS of its obligation to complete all work in accordance with the terms and conditions of this MOU.
17. CHILD AND DEPENDENT ADULT/ELDER ABUSE REPORTING
- MAXIMUS shall establish a procedure acceptable to COUNTY to ensure that all employees, agents, and all other individuals 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. MAXIMUS shall require such employees, agents, and all other individuals performing services under this MOU 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 shall comply with the provisions of these code sections, as they now exist or as they may hereafter be amended.

18. NOTICE TO EMPLOYEES REGARDING THE SAFELY SURRENDERED BABY LAW

MAXIMUS 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.

19. NOTICES

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

COUNTY: County of Orange Social Services Agency
Contracts Services
500 N. State College, Suite 100
Orange, CA 92868

MAXIMUS: Maximus, Inc.
Attn: Sara Summersett McGhee, Contracts Director
11050 Olson Drive, Suite 100
Rancho Cordova, CA 95670

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 communications, including notices, requests, claims, correspondence, reports, and/or statements authorized or required by this MOU, addressed in any other fashion shall be deemed not

given. The Parties each may designate by written notice from time to time, in the manner aforesaid, any change in the address to which notices must be sent.

20. RESOLUTION OF CONFLICTS

For resolution of conflicts between COUNTY and MAXIMUS in regard to the provisions of this MOU, the following shall apply:

Step 1: Conference between the Assistant Programs recipient's Case Manager and MAXIMUS Field Operations Director.

Step 2: Conference between the COUNTY Assistance Programs Human Services Manager, Sr. and/or Deputy Director or designee, and MAXIMUS Field Operations Director.

Step 3: Conference between the COUNTY Director of Assistance Programs or designee and the Senior Vice President of MAXIMUS.

Nothing in this Paragraph limits the rights of the Parties under Paragraph 23.

21. CONFLICT OF INTEREST

MAXIMUS shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with the best interests of the County. This obligation shall apply to MAXIMUS; MAXIMUS's employees, and agents associated with accomplishing work and services hereunder. MAXIMUS's efforts shall include, but not be limited to establishing precautions to prevent its employees, and agents from providing or offering gifts, entertainment, payments, loans, or other considerations which could be deemed to influence or appear to influence County staff or elected officers from acting in the best interests of the County.

22. POLITICAL ACTIVITY

MAXIMUS agrees that the funds provided herein shall not be used to promote, directly or indirectly, any political party, political candidate, or political activity, except as permitted by law.

23. TERMINATION

- 23.1 Either Party 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 include, but not limited to, any breach of this MOU, any partial misrepresentation whether negligent or willful, fraud on the part of MAXIMUS, discontinuance of the services for reasons within MAXIMUS's reasonable control, and repeated or continued violations of County ordinances unrelated to performance under this MOU that, in the reasonable opinion of COUNTY, indicate a willful or reckless disregard for County laws and regulations. Exercise by COUNTY of the right to terminate this MOU shall relieve COUNTY of all further obligations under this MOU.
- 23.2 This MOU may also be terminated by MAXIMUS without prior notice if:
- 23.2.1 Agreement number 17-94437 as referenced above in subparagraph 4.1 is terminated for any reason, or
- 23.2.2 The State of California directs Maximus to terminate this MOU.
- 23.3 For ninety (90) calendar days prior to the expiration date of this MOU, or upon notice of termination of this MOU ("Transition Period"), MAXIMUS agrees to cooperate with COUNTY in the orderly transfer of service responsibilities, case records, and pertinent documents. The Transition Period may be modified as agreed upon in writing by the Parties. During the Transition Period, services and data access shall continue to be made available to COUNTY without alteration. MAXIMUS also shall assist COUNTY in extracting and/or transitioning all data in the format determined by COUNTY.
- 23.4 In the event of termination of this MOU, cessation of business by MAXIMUS, or any other event preventing MAXIMUS from continuing to provide services, MAXIMUS shall not withhold the COUNTY data or refuse for any reason, to promptly provide to COUNTY the COUNTY data if requested to do so on such

media as reasonably requested by COUNTY, even if COUNTY is then or is alleged to be in breach of this MOU.

23.5 The obligations under this MOU utilize COUNTY resources, for which funding, or portions of funding, may be contingent upon the State and/or federal budget; receipt of funds from and/or obligation of funds by the State and/or Federal Government; and inclusion of sufficient funding for the services hereunder in the budget approved by the COUNTY's Board of Supervisors for each fiscal year covered by this MOU. If such approval, funding, or appropriations are not forthcoming, or are otherwise limited, COUNTY may terminate, reduce, or modify this MOU without penalty.

23.6 If any term, covenant, condition, or provision of this MOU or the application thereof is held invalid, void, or unenforceable, the remainder of the provisions in this MOU shall remain in full force and effect and shall in no way be affected, impaired, or invalidated thereby.

24. SIGNATURE IN COUNTERPARTS

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 Parties. MAXIMUS represents and warrants that the person executing this MOU on behalf of and for MAXIMUS is an authorized agent who has actual authority to bind MAXIMUS to each and every term, condition and obligation of this MOU and that all requirements of MAXIMUS have been fulfilled to provide such actual authority.

25. GENERAL PROVISIONS

25.1 Nothing herein contained shall be construed as creating the relationship of employer and employee, or principal and agent, between COUNTY and any participant participating in this program, or any of MAXIMUS's agents or employees.

25.2 This MOU, with its Attachments incorporated herein by reference, 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.

- 25.3 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.
- 25.4 MAXIMUS warrants that it and its Personnel, described in Paragraph 16 of this MOU, who are subject to individual registration and/or licensing requirements, have 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 MOU, and agrees to maintain, and require its Personnel to maintain, these licenses and permits in effect for the duration of this MOU. MAXIMUS must notify COUNTY within one (1) business day of any change in license or permit status (e.g., becoming expired, inactive, etc.).
- 25.5 In the performance of this MOU, MAXIMUS shall comply with all applicable laws and regulations of the United States, State of California, County of Orange, and 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.
- 25.6 In the performance of this MOU, MAXIMUS may neither delegate its duties or

obligations nor assign its rights, either in whole or in part, without the prior written consent of COUNTY. Any attempted delegation or assignment without prior written consent shall be void.

- 25.7 The various headings, numbers, and organization herein are for the purpose of convenience only and shall not limit or otherwise affect the meaning of this MOU.

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

DocuSigned by:
By: Hunter Fede
92A36486CCAT4FD...
Hunter Fede
<<Name>>
<<Title>> Legal Counsel
Maximus, Inc.

Dated: 5/24/2024 | 1:49:35 PM CDT

By: _____
Deputy Purchasing Agent
County of Orange, Social Services Agency

Dated: _____

Approved As To Form
SSA Counsel
County of Orange, California

DocuSigned by:
By: Carolyn Frost
D3AB98D76D0B425...
Carolyn Frost
Deputy County Counsel

Dated: 5/24/2024 | 1:20:58 PM PDT

Attachment A

SOCIAL SERVICES AGENCY POLICY AND PROCEDURE I 6: INFORMATION TECHNOLOGY SECURITY AND USAGE

I. PURPOSE

To protect the integrity of the Social Services Agency's (SSA) Information Technology (IT) infrastructure, ensure its availability, reliability, accessibility, and prevent unauthorized disclosure of Confidential Information, including Personally Identifiable Information (PII). Additionally, this policy defines required responsibilities for all users of the SSA information technology infrastructure and supplements the County of Orange Information Technology Policies.

II. DEFINITIONS

Confidential Information is defined as information that must be protected from unauthorized disclosure or public release. Examples include, but are not limited to the following:

1. Client case records
2. Employment Records
3. Payroll and other financial information
4. Other sensitive or business-related information that is not intended for wide distribution

Personally Identifiable Information (PII) is information 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, but are not limited to name, Social Security Number, Social Security benefit data, date of birth, official state or government issued driver's license, or identification number. PII is a subset of Confidential Information.

SSA Workforce Members include full-time, part-time, and extra-help County of Orange SSA employees, contracted staff, interns, volunteers, and all other authorized individuals with access to SSA's information technology infrastructure.

III. POLICY

SSA workforce members shall adhere to applicable SSA and County policies, including, but not limited to, the following: [County of Orange Information Technology Usage Policy](#), state and federal statutes including ([California Welfare and Institutions Code, Division 9, Part 2, Chapter](#)

5), and regulations relating to information technology security, privacy, and confidentiality of information as each may now exist or be amended in the future.

Unless within the scope of job responsibility, any use of Confidential Information will be considered a violation of this policy and will be subject to immediate revocation of the user's access to SSA network and associated applications. SSA workforce members may be subject to disciplinary action including suspension, termination, civil, and/or criminal prosecution for violating governing security and usage policies, statutes, and regulations (e.g., and the [County of Orange Information Technology Usage Policy \(Attachment I\)](#)).

All SSA workforce members shall:

1. Keep user Identification(s) (ID)/Username(s) and passwords confidential and secured at all times.
2. Never share username(s)/password(s).
3. Immediately change passwords and notify IT and the supervisor if an account has been compromised.
4. Limit usage of County data, systems, and equipment to currently assigned job duties and responsibilities.
5. County-issued IT equipment shall not be used outside the State of California without express supervisory permission.
6. Use County resources, such as data and information, for County business objectives only. Use of these resources for private or personal gain is prohibited and may be subject to administrative, civil, and criminal penalties (e.g., [California Penal Code, Section 502](#)).
7. Protect Confidential Information of clients/customers to prevent unauthorized disclosure. Only the minimum amount of Confidential Information necessary for business operations should be copied, downloaded, exported, or stored on any electronic device or in paper format. Any compromise of Confidential Information and/or PII shall be immediately reported to the supervisor.
8. Request software installations/downloads on SSA computers, laptops, tablets and other devices from an authorized agent of the OC Information Technology (OCIT) team. DO NOT INSTALL ANY software/application into County-issued devices. Requests can be submitted through the Service Now portal at https://ismcg.service-now.com/oc?id=oc_index or by calling the Central IT Service Desk at (844) 834-2449.

Note: pre-approved applications for County-issued cell phones can be downloaded from the Company Portal (Comp Portal) application without seeking approval from OCIT.

9. Seek permission from OCIT prior to copying a County-owned software/application.
10. Use County electronic communication systems for business use only; any personal use during nonworking hours shall be in strict compliance with policy and shall not disrupt or interfere with County operations or job responsibilities. If there is any doubt about whether an activity is appropriate, consult with your supervisor or manager.
11. Adhere to related SSA policies, including [P&P F21 Privacy and Security Incidents of Personally Identifying Information \(PII\) and Confidential Information](#) and [P&P D20 Remote Work](#).

IV. PROCEDURE

SSA Employees

The following steps shall be undertaken to ensure that the above policy is enforced to all SSA County employees. Prior to a new employee gaining access to Confidential Information, the SSA Human Resources (HR) representative or designee shall:

1. Provide new employees with access to the SSA I-6 Policy and Procedures document, the County of Orange Information Technology Usage Policy ([Attachment I](#)) with instructions for the new employee to read and sign the SSA Information Technology Security and Usage Agreement ([Attachment II](#)). Upon the new employee's signing of SSA Information Technology Usage Agreement form, the HR representative or designee shall sign the completed form to acknowledge receipt.
2. Have the new employee read and sign the Orange County Social Services Agency Confidentiality of Client Information ([Attachment III](#)).
3. Confirm the new employee has completely reviewed the SSA Information Security Rules of the Road ([Attachment IV](#)) located in the Training section of the SSA Intranet at <http://ocssa/intranet/ssa/Training>.
4. File the signed SSA Information Technology Usage Agreement ([Attachment II](#)), the signed Orange County Social Services Agency Confidentiality of Client Information ([Attachment III](#)) and documentation of completion of SSA Information Security Rules of the Road ([Attachment IV](#)) in the employee's personnel file.

SSA Contracted Employee, Volunteer, Intern, and All Other Non-County Employees

The supervisor of an SSA contracted employee, volunteer, intern, and all other non-County employees shall undertake the following steps to ensure the above policy is enforced. Prior to a workforce member gaining access to Confidential Information, provide them with the following documents to read:

1. Administrative Policies and Procedures Manual I-6 Information Technology Security and Usage. The new workforce member shall document that they have read, understand and will adhere to the policies stated in the SSA I-6 policy and procedures document by signing the document titled: “Agreement to Comply with the Orange County Social Services Agency Information Technology Security and Usage Policy” ([Attachment V](#)). This document also includes the SSA Confidentiality Agreement and serves as documentation of completion of the SSA Information Security Rules of the Road training presentation. This action must occur prior to a workforce member being provided with access to Confidential Information.

Maintain this signed “Agreement to Comply with the Orange County Social Services Agency Information Technology Security and Usage Policy” ([Attachment V](#)) for three years after the non-County workforce member separates from SSA.

2. County of Orange Information Technology Usage Policy ([Attachment I](#)).

If this workforce member requires access to the SSA network or databases (e.g., shared drives, Statewide Eligibility Determination System, Imaging System, Child Welfare Services/Case Management System, SSA Intranet, etc.), a copy of the signed “Agreement to Comply with the Orange County Social Services Agency Information Technology Security and Usage Policy” ([Attachment V](#)) shall be provided to SSA’s System Support Team and OCIT via the provisioning process. Network access will not be provided until this signed document is received.

V. ATTACHMENTS

- I. [County of Orange Information Technology Usage Policy](#)
 - II. [SSA Information Technology Security and Usage Agreement](#)
 - III. [Orange County Social Services Agency Confidentiality of Client Information](#)
 - IV. [Social Services Agency Information Security Rules of the Road](#)
 - V. [Agreement to Comply with the Orange County Social Services Agency Information Technology Security and Usage Policy](#)
-

VI. RELATED SSA POLICIES

1. [P&P F21 Privacy and Security Incidents of Personally Identifying Information \(PII\) and Confidential Information](#)
2. [P&P D20: Remote Work](#)

VII. REFERENCES

1. [California Welfare and Institutions Code, Division 9, Part 2, Chapter 5](#)

1. 2. [California Penal Code, Section 502](#)

ATTACHMENT B

SOCIAL SERVICES AGENCY POLICY AND PROCEDURE F 21: PRIVACY AND SECURITY INCIDENTS OF PERSONALLY IDENTIFIABLE INFORMATION (PII) AND CONFIDENTIAL INFORMATION

I. PURPOSE

To establish a process and guidelines for Social Services Agency (SSA) to report, document and investigate privacy and security incidents of Personally Identifiable Information (PII) and confidential information.

II. POLICY

Orange County Social Services Agency (OCSSA) workforce, volunteers and contractors/vendors shall comply with all applicable Federal and State laws, regulations, policies and procedure regarding the safeguarding of PII and confidential information and incident reporting protocols.

This policy applies to all data sources and systems with any PII and other forms of confidential information that staff access in the performance of their duties via any medium including electronic, paper, and verbal.

III. DEFINITIONS

Action Officer: Person responsible for ensuring the program rectifies any issues identified with a breach. In most cases, it will be the program or regional manager.

Authorized Persons: are employees of the Agency who meet the following criteria:

- Need to access PII and other forms of confidential information in order to perform their job duties;
- Have completed all required security and confidentiality training; and
- Have completed all required security certifications relevant to the data which are on file and available for review by an outside agency.

Breach: Refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII, whether electronic, paper, verbal or recorded.

Confidential Information: Information that must be protected from unauthorized disclosure or public release. Examples of Confidential Information include but are not limited to the following: client case records, employment records, payroll and other financial information and other sensitive or business-related information that is not intended for wide distribution.

Federal Tax Information (FTI): any data extracted from an individual's federal tax return (including attachments) that the Internal Revenue Service (IRS) provides to human services agencies under IRC §6103(l)(7). FTI is received from the following Income Earnings Verification System (IEVS) Reports:

- Annual IRS Asset Match (paper only) and
- Monthly Beneficiary Earnings Exchange Record (BEER) Match (paper only).

Lost PII or confidential information in any medium or format: All PII or confidential information in any medium or format that a Deputy Director or delegated SSA manager has confirmed is no longer in the physical possession or control of an Agency representative; has been electronically transmitted to an unauthorized recipient; and/or has been accessed by an unauthorized user. This does not include information that has been misplaced within the confines of secured Agency facilities.

Personally Identifiable Information (PII): Is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometrics records; and (2) any other information that can be used alone or when combined with other personal or identifying information that is linked or linkable to an individual, such as medical, educational, financial and employment information.

Medi-Cal Personally Identifiable Information (Medi-Cal PII): 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. Medi-Cal 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.

Security Incident: Attempted or successful unauthorized access, use, disclosure, modification, or destruction of information that compromises the security, confidentiality or integrity of the PII.

Information may be in electronic, hardcopy, or verbal form and may consist of a single piece of information and/or an entire information system, such as hard drive, portable computer storage medium, cell phones, tablets, or laptop computer.

Social Security Administration Personally Identifiable Information: Covers PII received from the following Income Eligibility Verification System (IEVS) Reports:

- Monthly BEER Match (paper only); Payment Verification System (PVS) Match (electronic only);

- Integrated Earning Clearance/Fraud Detection System (IFD) Match (electronic only);
- Deceased Persons Match (DPM; paper only); and
- Nationwide Prisoner Match (NPM; paper or electronic).

SSA Workforce: Refers to employees, contracted staff, volunteers, interns, trainees, and other persons whose work is under the direct control and oversight of SSA.

Unauthorized Access: A user who gains logical or physical access without permission, a business need or other lawful reason to a network, system, application, data, site or other resource.

IV. PROCEDURE

A. Detection:

1. OCSSA workforce members have the responsibility to monitor for and report any known or suspected privacy or security incidents, breaches, intrusion or unauthorized access, use, or disclosure of PII. Examples of incidents or breaches include, but are not limited to:

- a. Theft/Loss of PII or FTI.
- b. E-mail, texting or faxing PII to an unknown or unauthorized recipient
- c. Theft/Loss of unencrypted device (phones, laptops, thumb drives, etc.) containing PII.
- d. Employee accessing or searching data systems containing PII without a legitimate business need.
- e. Improper disposal of records containing PII, such as in a dumpster or recycle bins.

2. OCSSA staff shall immediately report privacy and security incidents by following the process identified under Reporting and Resolution, with guidance from State and Federal documents located in the Reference and Attachment Sections.

B. Reporting and Resolution:

1. Immediately upon identifying any suspected privacy or security incidents, breaches, intrusion or unauthorized access, use, or disclosure of PII, the SSA employee will

immediately notify their Regional/Program Manager/Admin Management Team, with a CC to their immediate Supervisor.

2. The Regional/Program Manager, upon receiving information about the privacy or security incident, will immediately submit a Privacy Incident Report (PIR) to the Quality Support Team (QST)/Custodian of Records (COR) at SSAcustodianofrecordsinbox@SSA.ocgov.com with a CC to their Deputy Division Director, via a secure email message with the subject line "Initial PIR [secure]". Each section of the PIR will be completed with as much information as available at the time of drafting. No PII should be included in the PIR.

3. Upon receipt of the PIR, the Quality Support Team will collaborate with the Regional/Program Manager to further identify any details necessary to better assess the incident.

4. Upon gathering this information, the Quality Support Team will then connect with the County Privacy Officer to identify next steps.

5. As determined to be required, the QST/COR shall advise the identified program point of contact ("Action Officer") to update the PIR to include any additional information required. a. If the incident meets any of the criteria noted in the County Significant Incident/ Claim Reporting Protocol, QST/COR shall draft a report containing the basic/concise facts and submit to the Chief Deputy Director with the PIR attached for review and submission to IncidentReport@ocgov.com.

6. QST/COR will serve as the Agency's point of contact for the County Privacy Officer and will communicate all applicable steps identified by the County Privacy Officer to the Action Officer.

a. The Action Officer will be responsible for coordinating all applicable activities required to notify and rectify the privacy/security issue that was identified.

i. Action Officers will be assigned and will vary depending on the program.

ii. Depending on the type of issue, the References Section provided below will provide more information on what actions are necessary to rectify the situation. Loss of Medi-Cal PII involves different steps than a loss of PII for other programs.

b. The Action Officer shall oversee the completion of the investigation of the privacy or security incident.

- c. The Action Officer shall oversee notification of individuals affected by the breach or unauthorized use/disclosure of Medi-Cal PII when notification is required.
- d. The Action Officer shall engage Human Resource Services, County Counsel, Risk Management, and/or the County Executive Office as needed to determine if internal processes, such as disciplinary action, are necessary.
- e. At the conclusion of the investigation and completion of all required notifications and consultations regarding necessary internal processes, the Action Officer will send the completed PIR that includes all required documentation from the investigation to QST/COR at the SSACustodianofrecordsinbox@SSA.ocgov.com with the subject line "Final PIR [secure]."
7. The County Privacy Officer will submit the final PIR to DHCS as required.
8. QST/COR will retain the final PIR for all incident types.

V. REFERENCES

Compliance of this policy shall be in accordance with the:

For Loss of Medi-Cal PII:

State of California Department of Health Care Services Privacy and Security Agreement
<https://www.dhcs.ca.gov/services/medi-cal/eligibility/letters/Documents/c19-16.pdf>

For Loss of all other program PII:

State of California Department of Social Services Privacy and Security Agreement
<https://cdss.ca.gov/Portals/9/ACL/2019/19-56E.pdf?ver=2019-07-02-071938-893>

For Loss of Federal Tax Information (FTI): [State of California Health and Human Services Agency Department of Social Services \(CDSS\) All County Letters No. 15-56](#)

[California SB 1386](#) Personal Information: Privacy

[California Civil Code 1798.29](#)

[Children and Family Services Division \(CFS Policy F-0105\), Confidentiality-CFS Client Records](#)

[California Department of Health Care Services Data Privacy Contact Information](#)

Attachment C

County of Orange Information Technology Security Provisions

All Contractors with access to County data and/or systems shall establish and maintain policies, procedures, and technical, physical, and administrative safeguards designed to (i) ensure the confidentiality, integrity, and availability of all County data and any other confidential information that the Contractor receives, stores, maintains, processes, transmits, or otherwise accesses in connection with the provision of the contracted services, (ii) protect against any threats or hazards to the security or integrity of County data, systems, or other confidential information, (iii) protect against unauthorized access, use, or disclosure of personal or County confidential information, (iv) maintain reasonable procedures to prevent, detect, respond, and provide notification to the County regarding any internal or external security breaches, (v) ensure the return or appropriate disposal of personal information or other confidential information upon contract conclusion (or per retention standards set forth in the contract), and (vi) ensure that any subcontractor(s)/agent(s) that receives, stores, maintains, processes, transmits, or otherwise accesses County data and/or system(s) is in compliance with statements and the provisions of statements and services herein.

1. County of Orange Information Technology Security Guidelines: County of Orange security standards follows the latest National Institute of Standards and Technology (NIST) 800-53 framework to ensure the highest levels of operational resiliency and cybersecurity.

Contractor, Contractor personnel, Contractor's subcontractors, any person performing work on behalf of Contractor, and all other agents and representatives of Contractor will, at all times, comply with and abide by all [County of Orange Information Technology Security Guidelines](#) ("Security Guidelines"), as existing or modified, that pertain to Contractor in connection with the Services performed by Contractor as set forth in the scope of work of this Memorandum of Understanding (MOU). Any violations of such Security Guidelines shall, in addition to all other available rights and remedies available to County, be cause for immediate termination of this MOU. Such Security Guidelines include, but are not limited to, Attachment C - County of Orange Information Technology Security Provisions and Attachment D – State Privacy and Security Provisions.

Contractor shall use industry best practices and methods with regard to confidentiality, integrity, availability, and the prevention, detection, response, and elimination of threat, by all appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to County data and/or system(s) accessed in the performance of Services under this MOU.

2. The Contractor shall implement and maintain a written information security program that contains reasonable and appropriate security measures designed to safeguard the confidentiality, integrity, availability, and resiliency of County data and/or system(s). The

Contractor shall review and update its information security program in accordance with contractual, legal, and regulatory requirements. Contractor shall provide to County a copy of the organization's information security program and/or policies.

3. Information Access: Contractor shall use appropriate safeguards and security measures to ensure the confidentiality and security of all County data.

County may require all Contractor personnel, subcontractors, and affiliates approved by County to perform work under this MOU to execute a confidentiality and non-disclosure agreement concerning access protection and data security in the form provided by County. County shall authorize, and Contractor shall issue, any necessary information-access mechanisms, including access IDs and passwords, and in no event shall Contractor permit any such mechanisms to be shared or used by other than the individual Contractor personnel, subcontractor, or affiliate to whom issued. Contractor shall provide each Contractor personnel, subcontractors, or affiliates with only such level of access as is required for such individual to perform his or her assigned tasks and functions.

Throughout the MOU term, upon request from County but at least once each calendar year, Contractor shall provide County with an accurate, up-to-date list of those Contractor personnel and/or subcontractor personnel having access to County systems and/or County data, and the respective security level or clearance assigned to each such Contractor personnel and/or subcontractor personnel. County reserves the right to require the removal and replacement of Contractor personnel and/or subcontractor personnel at the County's sole discretion. Removal and replacement shall be performed within 14 calendar days of notification by the County.

All County resources (including County systems), County data, County hardware, and County software used or accessed by Contractor: (a) shall be used and accessed by such Contractor and/or subcontractors personnel solely and exclusively in the performance of their assigned duties in connection with, and in furtherance of, the performance of Contractor's obligations hereunder; and (b) shall not be used or accessed except as expressly permitted hereunder, or commercially exploited in any manner whatsoever, by Contractor or Contractor's personnel and subcontractors, at any time.

Contractor acknowledges and agrees that any failure to comply with the provisions of this paragraph shall constitute a breach of this MOU and entitle County to deny or restrict the rights of such non-complying Contractor personnel and/or subcontractor personnel to access and use the County data and/or system(s), as County in its sole discretion shall deem appropriate.

4. Data Security Requirements: Without limiting Contractor's obligation of confidentiality as further described in this MOU, Contractor must establish, maintain, and enforce a data privacy program and an information and cyber security program, including safety, physical, and technical security and resiliency policies and procedures, that comply with the requirements set forth in this MOU and, to the extent such programs are consistent with and

not less protective than the requirements set forth in this MOU and are at least equal to applicable best industry practices and standards (NIST 800-53).

Contractor also shall provide technical and organizational safeguards against accidental, unlawful, or unauthorized access or use, destruction, loss, alteration, disclosure, transfer, commingling, or processing of such information that ensure a level of security appropriate to the risks presented by the processing of County Data,

Contractor personnel and/or subcontractor personnel and affiliates approved by County to perform work under this MOU may use or disclose County personal and confidential information only as permitted in this MOU. Any other use or disclosure requires express approval in writing by the County of Orange. No Contractor personnel and/or subcontractor personnel or affiliate shall duplicate, disseminate, market, sell, or disclose County personal and confidential information except as allowed in this MOU. Contractor personnel and/or subcontractor personnel or affiliate who access, disclose, market, sell, or use County personal and confidential information in a manner or for a purpose not authorized by this MOU may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

Contractor shall take all reasonable measures to secure and defend all locations, equipment, systems, and other materials and facilities employed in connection with the Services against hackers and others who may seek, without authorization, to disrupt, damage, modify, access, or otherwise use Contractor systems or the information found therein; and prevent County data from being commingled with or contaminated by the data of other customers or their users of the Services and unauthorized access to any of County data.

Contractor shall also continuously monitor its systems for potential areas where security could be breached. In no case shall the safeguards of Contractor's data privacy and information and cyber security program be less stringent than the safeguards used by County. Without limiting any other audit rights of County, County shall have the right to review Contractor's data privacy and information and cyber security program prior to commencement of Services and from time to time during the term of this MOU.

All data belongs to the County and shall be destroyed or returned at the end of the MOU via digital wiping, degaussing, or physical shredding as directed by County.

5. **Enhanced Security Measures:** County may, in its discretion, designate certain areas, facilities, or solution systems as ones that require a higher level of security and access control. County shall notify Contractor in writing reasonably in advance of any such designation becoming effective. Any such notice shall set forth, in reasonable detail, the enhanced security or access-control procedures, measures, or requirements that Contractor shall be required to implement and enforce, as well as the date on which such procedures and measures shall take effect. Contractor shall and shall cause Contractor personnel and

subcontractors to fully comply with and abide by all such enhanced security and access measures and procedures as of such date.

- 6. General Security Guidelines:** Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems, email systems, auditing, and monitoring systems) and networks used by or for Contractor (“Contractor Systems”) to access County resources (including County systems), County data or otherwise in connection with the Services and shall prevent unauthorized access to County resources (including County systems) or County data through the Contractor Systems.
- a) **Contractor System(s) and Security:** At all times during the MOU term, Contractor shall maintain a level of security with regard to the Contractor Systems, that in all events is at least as secure as the levels of security that are common and prevalent in the industry and in accordance with industry best practices (NIST 800-53). Contractor shall maintain all appropriate administrative, physical, technical, and procedural safeguards to secure County data from data breach, protect County data and the Services from loss, corruption, unauthorized disclosure, and from hacks, and the introduction of viruses, disabling devices, malware, and other forms of malicious and inadvertent acts that can disrupt County’s access and use of County data and the Services.
 - b) **Contractor and the use of Email:** Contractor, including Contractor’s employees and subcontractors, that are provided a County email address must only use the County email system for correspondence of County business. Contractor, including Contractor’s employees and subcontractors, must not access or use personal, non-County Internet (external) email systems from County networks and/or County computing devices. If at any time Contractor’s performance under this MOU requires such access or use, Contractor must submit a written request to County with justification for access or use of personal, non-County Internet (external) email systems from County networks and/or computing devices and obtain County’s express prior written approval.

Contractors who are not provided with a County email address, but need to transmit County data will be required to maintain and transmit County data in accordance with this Agreement.

- 7. Security Failures:** Any failure by the Contractor to meet the requirements of this MOU with respect to the security of County data, including any related backup, disaster recovery, or other policies, practices or procedures, and any breach or violation by Contractor or its subcontractors or affiliates, or their employees or agents, of any of the foregoing, shall be deemed a material breach of this MOU and may result in termination and reimbursement to

County of any fees prepaid by County prorated to the date of such termination. The remedy provided in this paragraph shall not be exclusive and is in addition to any other rights and remedies provided by law or under the MOU.

- 8. Security Breach Notification:** In the event Contractor becomes aware of any act, error or omission, negligence, misconduct, or security incident including unsecure or improper data disposal, theft, loss, unauthorized use and disclosure or access, that compromises or is suspected to compromise the security, availability, confidentiality, and/or integrity of County data or the physical, technical, administrative, or organizational safeguards required under this MOU that relate to the security, availability, confidentiality, and/or integrity of County data, Contractor shall, at its own expense, (1) immediately (or within 24 hours of potential or suspected breach), notify the County's Chief Information Security Officer and County Privacy Officer of such occurrence; (2) perform a root cause analysis of the actual, potential, or suspected breach; (3) provide a remediation plan that is acceptable to County within 30 days of verified breach, to address the occurrence of the breach and prevent any further incidents; (4) conduct a forensic investigation to determine what systems, data, and information have been affected by such event; and (5) cooperate with County and any law enforcement or regulatory officials investigating such occurrence, including but not limited to making available all relevant records, forensics, investigative evidence, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by County and/or any law enforcement or regulatory officials, and (6) perform or take any other actions required to comply with applicable law as a result of the occurrence (at the direction of County).

County shall make the final decision on notifying County officials, entities, employees, service providers, and/or the general public of such occurrence, and the implementation of the remediation plan. If notification to particular persons is required under any law or pursuant to any of County's privacy or security policies, then notifications to all persons and entities who are affected by the same event shall be considered legally required. Contractor shall reimburse County for all notification and related costs incurred by County arising out of or in connection with any such occurrence due to Contractor's acts, errors or omissions, negligence, and/or misconduct resulting in a requirement for legally required notifications.

In the case of a breach, Contractor shall provide third-party credit and identity monitoring services to each of the affected individuals for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than twelve (12) months following the date of notification to such individuals.

Contractor shall indemnify, defend with counsel approved in writing by County, and hold County and County Indemnitees harmless from and against any and all claims, including reasonable attorney's fees, costs, and expenses incidental thereto, which may be suffered by, accrued against, charged to, or recoverable from County in connection with the occurrence.

Notification shall be sent to:

Andrew Alipanah, MBA, CISSP
Chief Information Security Officer
1055 N. Main St., 6th Floor
Santa Ana, CA 92701
Phone: (714) 567-7611
Andrew.Alipanah@ocit.ocgov.com

Linda Le, CHPC, CHC, CHP
County Privacy Officer
1055 N. Main St., 6th Floor
Santa Ana, CA 92701
Phone: (714) 834-4082
Linda.Le@ocit.ocgov.com

County of Orange
Social Services Agency
Contracts Services
500 N. State College Blvd, Suite 100
Orange, CA 92868
714-541-7785
Karen.Vu@ssa.ocgov.com

- 9. Security Audits:** Contractor shall maintain complete and accurate records relating to its system and Organization Controls (SOC) Type II audits or equivalent's data protection practices, internal and external audits, and the security of any of County-hosted content, including any confidentiality, integrity, and availability operations (data hosting, backup, disaster recovery, external dependencies management, vulnerability testing, penetration testing, patching, or other related policies, practices, standards, or procedures). Contractor shall inform County of any internal/external security audit or assessment performed on Contractor's operations, information and cyber security program, disaster recovery plan, and prevention, detection, or response protocols that are related to hosted County content, within sixty (60) calendar days of such audit or assessment. Contractor will provide a copy of the audit report to County within thirty (30) days after Contractor's receipt of request for such report(s).

Contractor shall reasonably cooperate with all County security reviews and testing, including but not limited to penetration testing of any cloud-based solution provided by Contractor to County under this MOU. Contractor shall implement any required safeguards as identified by County or by any audit of Contractor's data privacy and information/cyber security program.

In addition, County has the right to review Plans of Actions and Milestones (POA&M) for any outstanding items identified by the SOC 2 Type II report requiring remediation as it pertains to the confidentiality, integrity, and availability of County data. County reserves the right, at its sole discretion, to immediately terminate this MOU or a part thereof without limitation and without liability to County if County reasonably determines Contractor fails or has failed to meet its obligations under this section.

10. Business Continuity and Disaster Recovery (BCDR):

For the purposes of this section, “Recovery Point Objectives” means the maximum age of files (data and system configurations) that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure (establishing the data backup schedule and strategy). “Recovery Time Objectives” means the maximum duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a loss of functionality.

The Contractor shall maintain a comprehensive risk management program focused on managing risks to County operations and data, including mitigation of the likelihood and impact of an adverse event occurring that would negatively affect contracted services and operations of the County. Business continuity management will enable the Contractor to identify and minimize disruptive risks and restore and recover hosted County business-critical services and/or data within the agreed terms following an adverse event or other major business disruptions. Recovery and timeframes may be impacted when events or disruptions are related to dependencies on third-parties. The County and Contractor will agree on Recovery Point Objectives and Recovery Time Objectives (as needed) and will periodically review these objectives. Any disruption to services of system will be communicated to the County within 4 hours, and every effort shall be undertaken to restore contracted services, data, operations, security, and functionality.

All data and/or systems and technology provided by the Contractor internally and through third-party vendors shall have resiliency and redundancy capabilities to achieve high availability and data recoverability. Contractor Systems shall be designed, where practical and possible, to ensure continuity of service(s) in the event of a disruption or outage.

Attachment D

State Privacy and Security Provisions

1. DEFINITIONS

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

- a. “**Assist in the Administration of the Program**” means performing administrative functions on behalf of programs, such as determining eligibility for, or enrollment in, and collecting PII for such purposes, to the extent such activities are authorized by law.
- b. “**Breach**” refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII, whether electronic, paper, verbal, or recorded.
- c. “**Contractor Staff**” means those employees of the contractor/subcontractor, vendors and agents performing any functions for the county that require access to and/or use of PII and that are authorized by the county to access and use PII.
- d. “**PII**” is personally identifiable information that is obtained through the MEDS or IEVS on behalf of the programs and can be used alone, or in conjunction with any other reasonably available information, to identify a specific individual. The PII includes, but is not limited to, an individual's name, social security number, driver's license number, identification number, biometric records, date of birth, place of birth, or mother's maiden name. The PII may be electronic, paper, verbal, or recorded.
- e. “**Security Incident**” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII, or interference with system operations in an information system which processes PII that is under the control of the county or county's Statewide Automated Welfare System (SAWS) Consortium, or CalSAWS (California Statewide Welfare System), or under the

control of a contractor, subcontractor or vendor of the county, on behalf of the county.

- f. "Secure Areas" means any area where:
- i. Contractor Staff assist in the administration of their program;
 - ii. Contractor Staff use or disclose PII; or
 - iii. PII is stored in paper or electronic format.

2. PRIVACY AND CONFIDENTIALITY

- a. The County staff, contractors, subcontractors and vendors, covered by this Agreement may use or disclose PII only as permitted in this Agreement and only to assist in the administration of programs in accordance with 45 CFR § 205.50 et seq. and Welfare and Institutions Code section 10850, and Section 14100.2 of the Welfare and Institutions Code, Section 431.300 et. Seq. of Title 42 Code of Federal Regulations, or as authorized or required by law. Disclosures, which are authorized or required by law, such as a court order, or are made with the explicit written authorization of the individual, who is the subject of the PII, are allowable. Any other use or disclosure of PII requires the express approval in writing by County of Orange. No Contractor Staff shall duplicate, disseminate or disclose PII except as allowed in this Agreement.
- b. Pursuant to this Agreement, Contractor Staff may only use PII to perform administrative functions related to administering their respective programs.
- c. Access to PII shall be restricted to Contractor Staff who need to perform their official duties to assist in the administration of their respective programs.
- d. Contractor Staff who access, disclose or use 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.

3. PERSONNEL CONTROLS

The County agrees to advise Contractor Staff, who have access to 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 Contractor shall implement the following personnel controls:

- a. **Employee Training.** Train and use reasonable measures to ensure compliance with the requirements of this Agreement by Contractor Staff, including, but not limited to:
 - i. Provide initial privacy and security awareness training to each new Contractor Staff within thirty (30) days of employment and;
 - ii. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this Agreement to all Contractor Staff. Three (3) or more security reminders per year are recommended;
 - iii. Maintain records indicating each Contractor Staff's name and the date on which the privacy and security awareness training was completed;
 - iv. Retain training records for a period of three (3) years after completion of the training.
- b. **Employee Discipline.**
 - i. Provide documented sanction policies and procedures for Contractor Staff who fail to comply with privacy policies and procedures or any provisions of these requirements.
 - ii. Sanction policies and procedures shall include termination of employment when appropriate.
- c. **Confidentiality Statement.** Ensure that all Contractor Staff, accessing, using or disclosing PII, sign a confidentiality statement (provided by the County). The statement shall be signed by Contractor staff prior to accessing PII and annually thereafter. Signatures may be physical or electronic. The signed statement shall be retained for a period of three (3) years.
The statement shall include at a minimum:
 - i. General Use;
 - ii. Security and Privacy Safeguards;
 - iii. Unacceptable Use; and

iv. Enforcement Policies.

d. **Background Screening.**

- i. Conduct a background screening of a Contractor Staff before they may access PII.
- ii. The background screening should be commensurate with the risk and magnitude of harm the employee could cause. More thorough screening shall be done for those employees who are authorized to bypass significant technical and operational security controls.
- iii. The Contractor shall retain each Contractor Staff's background screening documentation for a period of three (3) years following conclusion of employment relationship.

4. **MANAGEMENT OVERSIGHT AND MONITORING**

To ensure compliance with the privacy and security safeguards in this Agreement the County shall perform the following:

- a. Conduct periodic privacy and security reviews of work activity by Contractor Staff, including random sampling of work product. Examples include, but are not limited to, access to case files or other activities related to the handling of PII.
- b. The periodic privacy and security reviews must be performed or overseen by management level personnel who are knowledgeable and experienced in the areas of privacy and information security in the administration of their program, and the use or disclosure of PII.

5. **INFORMATION SECURITY AND PRIVACY STAFFING**

The Contractor 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. Provide County with applicable contact information for these designated individuals. Any changes to this information should be reported to County within ten (10) days.
- c. Assign staff to be responsible for administration and monitoring of all security related controls stated in this Agreement.

6. **PHYSICAL SECURITY**

The Contractor shall ensure PII is used and stored in an area that is physically safe from access by unauthorized persons at all times. The Contractor agrees to safeguard PII from loss, theft, or inadvertent disclosure and, therefore, agrees to:

- a. Secure all areas of the Contractor's facilities where Contractor Staff assist in the administration of their program and use, disclose, or store PII.
- b. These areas shall be restricted to only allow access to authorized individuals by using one or more of the following:
 - i. Properly coded key cards
 - ii. Authorized door keys
 - iii. Official identification
- c. Issue identification badges to Contractor Staff.
- d. Require Contractor Staff to wear these badges where PII is used, disclosed, or stored.
- e. Ensure each physical location, where PII is used, disclosed, 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.
- f. Ensure there are security guards or a monitored alarm system at all times at the Contractor facilities and leased facilities where five hundred (500) or more individually identifiable records of PII is used, disclosed or stored. Video surveillance are recommended.
- g. Ensure data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter

security and physical access controls that limit access to only authorized Contractor Staff. Visitors to the data center area must be escorted at all times by authorized Contractor Staff.

- h. Store paper records with PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which have multi-use functions in one building in work areas that are not securely segregated from each other. It is recommended that all PII be locked up when unattended at any time, not just within multi-use facilities.
- i. The Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which the Contractor Staff can transport PII, as well as the physical security requirements during transport. A Contractor that chooses to permit its staff to leave records unattended in vehicles must include provisions in its policies to ensure the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.
- j. The Contractor shall have policies that indicate Contractor Staff are not to leave records with PII unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.
- k. Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing PII.

7. TECHNICAL SECURITY CONTROLS

- a. **Workstation/Laptop Encryption.** All workstations and laptops, which use, store and/or process PII, must be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.
- b. **Server Security.** Servers containing unencrypted PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the

guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

- c. **Minimum Necessary.** Only the minimum necessary amount of PII required to perform required business functions may be accessed, copied, downloaded, or exported.
- d. **Mobile Device and Removable Media.** All electronic files, which contain PII data, must be encrypted when stored on any mobile device or removable media (i.e., USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.
- e. **Antivirus Software.** All workstations, laptops and other systems, which process and/or store PII, must install and actively use an antivirus software solution. Antivirus software should have automatic updates for definitions scheduled at least daily.
- f. **Patch Management.**
 - i. All workstations, laptops and other systems, which process and/or store PII, must have critical security patches applied, with system reboot if necessary.
 - ii. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.
 - iii. At a maximum, all applicable patches deemed as critical must be installed within thirty (30) days of vendor release. It is recommended that critical patches which are high risk be installed within seven (7) days.
 - iv. 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.**
 - i. All users must be issued a unique username for accessing PII.

- ii. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee within twenty-four (24) hours. Note: Twenty-four (24) hours is defined as one (1) working day.
- iii. Passwords are not to be shared.
- iv. Passwords must be at least eight (8) characters.
- v. Passwords must be a non-dictionary word.
- vi. Passwords must not be stored in readable format on the computer or server.
- vii. Passwords must be changed every ninety (90) days or less.
- viii. Passwords must be changed if revealed or compromised.
- ix. Passwords must be composed of characters from at least three (3) of the following four (4) groups from the standard keyboard:
 - A. Upper case letters (A-Z)
 - B. Lower case letters (a-z)
 - C. Arabic numerals (0-9)
 - D. Special characters (!,@,#, etc.)
- h. **Data Destruction.** When no longer needed, all PII must be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the PII cannot be retrieved.
- i. **System Timeout.** The systems providing access to PII must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.
- j. **Warning Banners.** The systems providing access to PII must display a warning banner stating, at a minimum:
 - i. Data is confidential;
 - ii. Systems are logged;
 - iii. System use is for business purposes only, by authorized users; and
 - iv. Users shall log off the system immediately if they do not agree with these requirements.
- k. **System Logging.**

- i. The systems which provide access to PII must maintain an automated audit trail that can identify the user or system process which initiates a request for PII or alters PII.
 - ii. The audit trail shall:
 - A. Be date and time stamped;
 - B. Log both successful and failed accesses;
 - C. Be read-access only; and
 - D. Be restricted to authorized users.
 - iii. If PII is stored in a database, database logging functionality shall be enabled.
 - iv. Audit trail data shall be archived for at least three (3) years from the occurrence.
- l. **Access Controls.** The system providing access to PII shall use role-based access controls for all user authentications, enforcing the principle of least privilege.
- m. **Transmission Encryption.**
- i. All data transmissions of PII outside of a secure internal network must be encrypted using a Federal Information Processing Standard (FIPS) 140-2 certified algorithm that is 128 bit or higher, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS). It is encouraged, when available and when feasible, that 256 bit encryption be used.
 - ii. Encryption can be end to end at the network level, or the data files containing PII can be encrypted.
 - iii. This requirement pertains to any type of PII in motion such as website access, file transfer, and email.
- n. **Intrusion Prevention.** All systems involved in accessing, storing, transporting, and protecting PII, which are accessible through the Internet, must be protected by an intrusion detection and prevention solution.

8. AUDIT CONTROLS

- a. **System Security Review.**
 - i. The Contractor must ensure audit control mechanisms are in place.
 - ii. All systems processing and/or storing 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 level of protection.
 - iii. Reviews should include vulnerability scanning tools.
- b. **Log Reviews.** All systems processing and/or storing PII must have a process or automated procedure in place to review system logs for unauthorized access.
- c. **Change Control.** All systems processing and/or storing PII must have a documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.
- d. **Anomalies.** When the County or DHCS suspects MEDS usage anomalies, the County will work with Contractor to investigate the anomalies and report conclusions of such investigations and remediation to California Department of Social Services (CDSS).

9. **BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS**

- a. **Emergency Mode Operation Plan.** The Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of 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 twenty-four (24) hours.
- b. **Data Centers.** Data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of PII, must include environmental protection such as cooling, power, and fire prevention, detection, and suppression.
- c. **Data Backup and Recovery Plan.**

- i. The Contractor shall have established documented procedures to backup PII to maintain retrievable exact copies of PII.
- ii. The documented backup procedures shall contain a schedule which includes incremental and full backups.
- iii. The procedures shall include storing backups offsite.
- iv. The procedures shall ensure an inventory of backup media.
- v. The Contractor shall have established documented procedures to recover PII data.
- vi. The documented recovery procedures shall include an estimate of the amount of time needed to restore the PII data.
- vii. It is recommended that the Contractor periodically test the data recovery process.

10. **PAPER DOCUMENT CONTROLS**

- a. **Supervision of Data.** The 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 may be observed by an individual not authorized to access the information.
- b. **Data in Vehicles.** The Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which the Contractor Staff can transport PII, as well as the physical security requirements during transport. A Contractor that chooses to permit its staff to leave records unattended in vehicles must include provisions in its policies to ensure the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.
- c. **Public Modes of Transportation.** The PII in paper form shall not be left unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.

- d. **Escorting Visitors.** Visitors to areas where PII is contained shall be escorted, and PII shall be kept out of sight while visitors are in the area.
- e. **Confidential Destruction.** PII must be disposed of through confidential means, such as cross-cut shredding or pulverizing.
- f. **Removal of Data.** The PII must not be removed from the premises of Contractor except for identified routine business purposes or with express written permission of HHS.
- g. **Faxing.**
 - i. Faxes containing PII shall not be left unattended and fax machines shall be in secure areas.
 - ii. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.
 - iii. Fax numbers shall be verified with the intended recipient before sending the fax.
- h. **Mailing.**
 - i. Mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.
 - ii. Mailings that include five hundred (500) or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt, unless the Contractor obtains prior written permission from HHS to use another method.

11. **NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS**

During the term of this Agreement, the County 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 HHS:

- i. The Contractor will provide initial notice to the County. The Contractor agrees to perform the following incident reporting to County.
 - ii. Immediately upon discovery of a suspected security incident that involves data provided to Contractor by County, the Contractor will notify the County by email or telephone.
 - iii. Within one working day of discovery, the Contractor will notify the County by email or telephone of unsecured PII, if that PII was, or is, reasonably believed to have been accessed or acquired by an unauthorized person, any suspected security incident, intrusion, or unauthorized access, use, or disclosure of PII in violation of this Agreement, or potential loss of confidential data affecting this Agreement. Notice shall be made by contacting the County as provided in this agreement, including all information known at the time.
 - iv. A breach shall be treated as discovered by the Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach), who is an employee, officer or other agent of the Contractor.
 - v. Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII, the Contractor shall take:
 - A. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
 - B. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
- b. Investigation and Investigative Report. The Contractor shall immediately investigate breaches and security incidents involving PII. The Contractor will cooperate with the County during this investigation. Within seventy-two (72) hours of discovery, the Contractor shall provide new or updated information if available to County. The updated report shall include any other applicable information related to the breach or security incident known at that time. The Contractor shall provide status update to County on a regular basis as agreed upon.

The Contractor shall provide to County all specific and pertinent information about the Breach, including copies of any reports conducted by the Contractor or on behalf of the Contractor. The Contractor shall waive any assertion of privilege in relation to such reports. Such information and/or reports shall be provided to County without unreasonable delay and in no event later than fifteen (15) calendar days the Contractor have such information and/or report.

- c. **Complete Report.** The complete report of the investigation shall include an assessment of all known factors relevant to the determination of whether a breach occurred under applicable provisions of the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Information Protection Act, or other applicable law. The report shall include a Corrective Action Plan (CAP) which includes, at a minimum, detailed information regarding the mitigation measures taken to halt and/or contain the improper use or disclosure.

If County requests additional information related to the incident, the Contractor shall make reasonable efforts to provide County with such information. County will review report and determine whether a breach occurred and whether individual notification is required. County will maintain the final decision making over a breach determination.

- d. **Notifications of Individuals.** When applicable state or federal law requires notification to individuals of a breach or unauthorized disclosure of their PII, the County will make the decision to either notify clients or have the Contractor give notice. If the Contractor shall give the notice, it would be subject to the following provisions:
- i. If the cause of the breach is attributable to the Contractor or its subcontractors, agents or vendors, the Contractor shall pay any costs of such notifications, as well as any and all costs associated with the breach. If there are any questions as to whether the County or the Contractor is responsible for the breach, the County and the Contractor shall jointly determine responsibility for purposes of allocating the costs;

- ii. All notifications (regardless of breach status) regarding the beneficiaries' PII shall comply with the requirements set forth in Section 1798.29 of the California Civil Code and Section 17932 of Title 42 of the United States Code, inclusive of its implementing regulations, including but not limited to the requirement that the notifications be made without reasonable delay and in no event, later than sixty (60) calendar days from discovery;
 - iii. The County has contractual requirement with the California Department of Social Services and California Department of Health Care Services to approve the time, manner and content of any such notifications and their review and approval shall be obtained before notifications are made. Therefore, the Contractor must provide the notifications to County to obtain review and approval prior to notifications are made. If notifications are distributed without State review and approval, secondary follow-up notifications may be required; and
 - iv. The County may elect to assume responsibility for such notification from the Contractor.
- e. **Responsibility for Reporting of Breaches when Required by State or Federal Law.** If the cause of a breach is attributable to the Contractor or its agents, subcontractors or vendors, the Contractor is responsible for all required reporting of the breach. If the cause of the breach is attributable to the County, the County is responsible for all required reporting of 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 (Department of Health Care Services) and COSS (California Department of Social Services) (if the breach involves MEDS or SSA data), then the Contractor shall coordinate with the County 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. **County Contact Information.** The Contractor shall utilize the below contact information to direct all notifications of breach and security incidents to the County. The County reserves the right to make changes to the contact information

by giving written notice to the Contractor. Said changes shall not require an amendment to this Agreement or any other agreement into which it is incorporated.

The preferred method of communication is email, when available. Do not include any Medi-Cal PI/PII unless requested by County.

SSA Contract Analyst	County Privacy Officer
County of Orange Social Services Agency Contracts Services 500 N. State College Blvd, Suite 100 Orange, CA 92868 <i>Attn: Contract Administrator</i>	Linda Le, CHC, CHPC, CHP County of Orange OCIT - Enterprise Privacy & Cybersecurity 1055 N. Main St, 6th Floor Santa Ana, CA 92701 Email: privacyofficer@ocgov.com securityadmin@ocit.ocgov.com linda.le@ocit.ocgov.com Telephone: (714) 834-4082

12. COMPLIANCE WITH SSA (SOCIAL SECURITY ADMINISTRATION) AGREEMENT

The County has agreed to comply with applicable privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency (CHHS), in the Information Exchange Agreement (IEA) between SSA and COSS, and in the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA (TSSR). If Contractor has access to the PII data provided by SSA, then Contractor must agree to comply with the applicable privacy and security requirements, which is available upon request.

If there is any conflict between a privacy and security standard in the CMPPA, IEA or TSSR, 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 PII.

13. COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY AGREEMENT

The County has agreed to comply with substantive privacy and security requirements in the Computer Matching Agreement (CMA) between the Department/Agency of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and CDSS. If Contractor has access to the PII data provided by DHS-USCIS, then Contractor must agree to comply with the applicable privacy and security requirements, which is available upon request.

If there is any conflict between a privacy and security standard in the CMA 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 PII.

14. CONTRACTOR AGENTS, SUBCONTRACTORS, AND VENDORS

The Contractor agrees to enter into written agreements with all agents, subcontractors, and vendors that have access to the Contractor's PII. These agreements will impose, at a minimum, the same restrictions and conditions that apply to the Contractor with respect to PII upon such agents, subcontractors, and vendors. These shall include, at a minimum, (1) restrictions on disclosure of PII, (2) conditions regarding the use of appropriate administrative, physical, and technical safeguards to protect PII, and, where relevant, (3) the requirement that any breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII be reported to the Contractor. If the agents, subcontractors, and vendors of the Contractor access data provided to the County by SSA or DHS-USCIS,

the Contractor shall also incorporate the Agreement's Attachments into each subcontract or subaward with agents, subcontractors, and vendors.

15. ASSESSMENTS AND REVIEWS

In order to enforce this Agreement and ensure compliance with its provisions, the Contractor agrees to assist the County (on behalf of COSS and DHCS) in performing compliance assessments. These assessments may involve compliance review questionnaires, and/or review of the facilities, systems, books, and records of the Contractor, with reasonable notice from the County. Such reviews shall be scheduled at times that take into account the operational and staffing demands. The Contractor agrees to promptly remedy all violations of any provision of this Agreement and certify the same to the County in writing, or to enter into a written CAP (Corrective Action Plan) with the County containing deadlines for achieving compliance with specific provisions of this Agreement.

16. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

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

Attachment E
License Agreement
(See Separate Attachment)