

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



ITEM: 3.18
(ID # 14476)

MEETING DATE:
Tuesday, March 09, 2021

FROM: PUBLIC SOCIAL SERVICES:

SUBJECT: DEPARTMENT OF PUBLIC SOCIAL SERVICES (DPSS): Approve the Professional Services Agreement # DPSS-0002444 with JUMP Technology Services, L.L.C. for an Adult Protective Services (APS) Case Management System, without seeking competitive bids, for 5 years effective on July 1, 2021 through June 30, 2026. All Districts; [Total Cost \$840,000 and up to \$33,600 in Additional Annual Compensation Provisions] – 26.33% Federal, 19.05% State, 10.58% County, 37.60% Realignment, 6.43% 2011 Realignment]

RECOMMENDED MOTION: That the Board of Supervisors:

1. Approve the Professional Services Agreement # DPSS-0002444 with JUMP Technology Services, L.L.C. for an APS Case Management System, without seeking competitive bids, for a total aggregate amount of \$840,000 through June 30, 2026, and authorize the Chair of the Board to sign the Agreement on behalf of the County; and
2. Authorize the Purchasing Agent, in accordance with Ordinance No. 459, based on the availability of fiscal funding and as approved as to form by County Counsel to: (a) sign amendments that make modifications to the scope of services that stay within the intent of the agreement; (b) sign amendments to the compensation provisions that do not exceed the sum total of twenty percent (20%) of the total annual cost of the agreement.

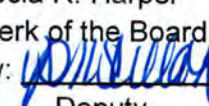
ACTION: Policy


Sayori Baldwin, DPSS Director 2/17/2021

MINUTES OF THE BOARD OF SUPERVISORS

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

Ayes: Jeffries, Spiegel, Washington, Perez, and Hewitt
Nays: None
Absent: None
Date: March 9, 2021
xc: DPSS

Kecia R. Harper
Clerk of the Board
By: 
Deputy

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

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost
COST	\$ 0	\$ 168,000	\$ 840,000	\$ 0
NET COUNTY COST	\$ 0	\$ 17,774	\$ 88,872	\$ 0
SOURCE OF FUNDS: 26.33% Federal, 19.05% State, 10.58% County, 37.60% Realignment, 6.43% 2011 Realignment			Budget Adjustment:	No
			For Fiscal Year:	21/22 - 25/26

C.E.O. RECOMMENDATION: Approve.

BACKGROUND:

Summary

JUMP Technology Services has been providing software maintenance to DPSS for APS related data via the LEAPS Case Management System since 2016. JUMP provides a cloud-based case management system as a Software-as-a-Service (SaaS). This software is proprietary and only JUMP can perform enhancements or modifications to the APS LEAPS system.

APS Social Workers receive and respond to reports of dependent and elder adult abuse then enter this information into the LEAPS database for Riverside County. The system serves 49 of California's 58 counties and offers features for cross reporting to another LEAPS county. System users can generate a cross report which appears in the receiving county's intake list. This is an important feature for programs to increase the accuracy of cross reported information. Other counties are often able to provide history on alleged victims, which is essential in serving the transient and homeless populations.

In addition, the LEAPS system provides social workers with contact information for family members of an alleged victim who may have a case in another jurisdiction. LEAPS is the only system that provides this feature. JUMP also offers smart mobile data captures that allow for APS Social Workers to collect client data out in the field. This unique feature is easy to support and proves that instant data capture leads to better performance.

As a Home Safe grant awardee, Riverside County can automate data collection and reporting features to meet CDSS' Home Safe requirements, created by Assembly Bill (AB) 1811 (Chapter 35, Statutes of 2018). The Adult Services Division (ASD) can request system enhancements that conform to the department's regulatory and procedural requirements. JUMP offers support 24 hours a day, 7 days a week, each day of the year.

Impact on Residents and Businesses

The LEAPS system provides APS with a comprehensive information management solution to ensure the health and safety of elder and dependent adults throughout Riverside County. APS is required to provide a system of in-person response, 24-hours a day, 7 days a week.

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

Additional Fiscal Information

ASD has averaged 312 licenses annually over the duration of the agreement. As part of the service package and annual cost, JUMP has included 60 service hours for custom query writing, custom reporting, and system modifications/enhancements. The budget is as follows:

Description:	FY21/22	FY22/23	FY23/24	FY24/25	FY25/26	Aggregate Total
User Subscriptions	\$150,500	\$150,500	\$150,500	\$150,500	\$150,500	\$752,500
Enhancement Budget	\$17,500	\$17,500	\$17,500	\$17,500	\$17,500	\$87,500
Total Costs	\$168,000	\$168,000	\$168,000	\$168,000	\$168,000	\$840,000

Contract History and Price Reasonableness

On December 29, 2015 DPSS entered into contract with JUMP Technology Services, L.L.C. for APS Case Management Services. These services were competitively bid, and the agreement was awarded to JUMP Technology Services, L.L.C. through RFQ DPARC-466. In addition, the Riverside County Information Technology Department approved the purchase of this software on November 6, 2014 via Procurement Form # PR2014-02061.

JUMP offers expertise in devising innovative Health and Human Services solutions and provides a unique mix of prebuilt system modules that leverages the efficiency of custom APS software. In addition to the many case management features, JUMP Technology is now hosting its services in a FedRAMP certified cloud environment, which provides assurance to the County's I.T. and the security of PII level information. Data centers are strategically placed in FedRAMP-authorized locations and JUMPs private cloud architecture permits government entities to meet all organization-specific security requirements.

ATTACHMENTS:

Attachment A: Professional Services Agreement DPSS-0002444 with JUMP Technology Services, L.L.C.


Tina Grande, Director of Purchasing 2/23/2021


Gregory V. Priamos, Director County Counsel 2/23/2021



Use this form to submit a single or sole source requisition for review by your Buyer and/or Procurement Contract Specialist. All procurements valued **\$5,000 or more** must seek competitive bids from a minimum of three suppliers, or the expectation that three or more suppliers will respond, or be justified by a Single/Sole Source. All purchases exceeding **\$50,000** require a formal public bid. Procurement's may not be artificially segregated to lesser dollar amounts for the purpose of bypassing this requirement.

Sole/Single Source service requests that are greater than **\$50,000** require additional Board of Supervisors approval.

Supplier Details

Vendor JUMP Technology Services LLC
Fulfillment Address LLCp - Services: (preferred)
 200 Russell M Perry Ave
 Oklahoma City, OK 73104 US

Distribution

The system will distribute purchase orders using the method(s) indicated below;
 Check this box to customize order distribution information. ✓
 Contract

Background Information

Please indicate if this is a single or sole source below

Single Source

Have you previously requested and received approval for a sole/single source request for this vendor for your department?

No

If selected "yes", please provide the approved SSJ# below

SSJ#

If selected "yes", was the request approved for a different project?

Purchase Details

1. Supply/Service being requested:

JUMP Technology Services, L.L.C. has been a leader in providing information technology products and services to public agencies and organizations for more than 30 years. With expertise in devising innovative Health and Human Services solutions, JUMP offers a unique mix of prebuilt system modules that allows DPSS to leverage the efficiency of custom APS software. The Adult Services Division is requesting continued support from JUMP Technology Services for APS Case Management Software.

On December 29, 2015 DPSS entered into contract with JUMP Technology Services L.L.C. for APS Case Management Services.

Current Year Cost

6. Identify all costs for this requested purchase.

You do not need to include previous fiscal year amounts. If approval is for multiple years, ongoing costs must be identified below. If annual increases apply to ongoing costs such as CPI or other contract increases, provide the estimated annual cost for each consecutive year. If the annual increase may exceed the Purchasing Agent's authority, Board approval must be obtained.

These services were competitively bid, and the agreement was awarded to JUMP Technology Services through RFQ DPARC-466.

2. Unique features of the supply/service being requested from this supplier, which no alternative supplier can provide:

Since 2016, JUMP Technology has been providing software maintenance to DPSS for APS related data via the LEAPS Case Management System. JUMP provides a cloud-based case management system as a Software-as-a-Service (SaaS). As such, it is proprietary and only JUMP can perform enhancements or modifications to the APS LEAPS system.

In addition to the many case management features, JUMP Technology is now hosting its services in a FedRAMP certified cloud environment. This will provide assurance to the County's I.T. and the security of PII. Data centers are strategically placed in FedRAMP-authorized locations and JUMPs private cloud architecture allows government entities to meet all NIST 800-53, FISMA, FedRAMP and organization-specific security requirements.

JUMP also provides smart mobile data captures that allow APS Social Workers to collect client data out in the field. This unique feature is easy to support and proves that instant data capture leads to better performance.

3. Reasons why my department requires these unique features and what benefit will accrue to the county:

LEAPS, a software as a service solution for Adult Protective Services provides a comprehensive information management solution. The purchase of the LEAPS Case Management System is required to ensure the health and safety of elder and dependent adults throughout Riverside County. APS provides a system of in-person response, 24-hours a day, 7 days a week. APS Social Workers receive and respond to reports of dependent adult and elder abuse in Riverside County and enter this information into the LEAPS database. The LEAPS system allows APS staff to utilize a streamlined process to capture the decision markers and scoring of the SDM intake resulting to the investigation being screened out or assigned to staff as a case investigation. The integration prevents duplication of effort while allowing APS to reflect accuracy in community reporting counts.

The goal of APS is to intervene and assist elder or dependent adults to alleviate physical, sexual and financial abuse, neglect, isolation and abandonment, abduction and mental suffering. Adult Protective Services operates under California's Welfare and Institutions Code 15640 and LEAPS provides functionality that complies specifically with this code. The LEAPS system automatically generates the following:

Describe all current fiscal year costs associated with this procurement in the box below. Insert all one time costs associated with this project in the table below.

There is no dollar amount associated with the current FY 20/21.

Insert all current fiscal year costs in the table below. Label the 'description' as the item that is being purchased.

Current FY Costs

Description	Price
APS Case Management Services	0.00

Enter all additional FY costs in the table below . Only enter one fiscal year cost per line and identify the fiscal year that it pertains to. Fiscal year is from 7/1/00 to 6/30/00.. Example : FY 18/19 \$200

FY	FY 20/21 \$0.00
FY	FY 21/22 \$168,000
FY	FY 22/23 \$168,000
FY	FY 23/24 \$168,000
FY	FY 24/25 \$168,000
Additional FY Cost	FY 25/26 \$168,000

Describe all additional costs associated with this procurement in the box below. Include the dollar amounts for subsequent fiscal years if it differs from above.

Current Year Cost Total: 0.00

1. SOC 341 for reports of abuse, neglect, and exploitation
2. SOC 342 for financial exploitation reports
3. SOC 343 investigative report
4. SOC 242 monthly statistical reporting form

In addition to these required outputs, LEAPS offers features for cross reporting to another LEAPS county. The system serves 49 of California's 58 counties. LEAPS system users can generate a cross report which appears in the receiving county's intake list. The receiving county can view the name of the county who sent the report. This is an important feature for programs to increase the accuracy of the cross reported information.

4. Period of Performance 7/1/2021

From:

Period of Performance To: 6/30/2026

Is this an annually renewable contract or is it fixed term?

Fixed Term

5. Price Reasonableness:

JUMP Technology is now hosting their services in a secured FedRAMP cloud environment, which resulted to the organization increasing their costs by 25% annually. This cost increase applied to customers is to account for the expenses associated with implementing and maintaining the secured platform.

The standard cost for user licenses ranging from 300 to 350 users is \$279,000 per year. ASD has averaged 312 licenses annually over the duration of the previous agreement. JUMP agreed to discount the annual cost to \$150,500 for Riverside County to reflect their appreciation for the continued partnership. Riverside County's APS caseload is expected to grow based on the projection that the County will experience the highest percentage increase in California's elderly population aged 60 and over; this will result to an increase in staff and user licenses for the LEAPS system. The annual cost of \$150,500 also includes the following services:

- o 300-350 User Licenses
- o A dedicated training system hosted for Riverside County
- o Weekly database backups
- o 60 service hours for custom query writing, custom reporting, and system modifications/enhancements
- o 12 hours custom training per year

The enhancement budget is based on an hourly rate of \$125.00. According to the U.S. Bureau of Labor Statistics, the Consumer Price Index (CPI) inflation over the past five years has been 11% for Professional Services. In addition, the CPI is projected to increase 2.1% annually over the next 5 years. As part of the service package and annual cost, JUMP has included 60 services hours for custom query writing, custom reporting, and system

modifications/enhancements (totaling \$7,500). Historically, ASD has exceeded these hours to accommodate system enhancements relating to online APS intakes, reporting party software bugs, and new features. ASD is forecasting a slight increase for the enhancement budget due to projected system modifications and an increase in user caseload.

Projected Board of Supervisor Date (if applicable):

Commodity Code 96258

Supporting Documentation

If this request is for professional services, attach the service agreement to this sole source request. The Purchasing Agent, or designee, is the signing authority for agreements unless the service is exempted by Ordinance 459, Board delegated authority or by State law.

- Additional supporting documentation includes:
- Previously approved SSJ's
 - other

For all other requests, attach the vendor's cost proposal

Internal Attachments

Purchasing Approval

	Approved by	Date Approved	Approval Conditions/Comments
This section to be filled out by Purchasing Management only upon approval.	Suzanna Hinckley	1/29/2021	

Total 0.00

**County of Riverside Department of Public Social Services
Contracts Administration Unit
10281 Kidd Street
Riverside, CA 92503**

and

**JUMP Technology Services, L.L.C.
Software Management Services
DPSS-0002444**



TABLE OF CONTENTS

- 1. DEFINITIONS 4
- 2. DESCRIPTION OF SERVICES 5
- 3. PERIOD OF PERFORMANCE 5
- 4. COMPENSATION 5
- 5. AVAILABILITY OF FUNDS/NON-APPROPRIATION OF FUNDS 5
- 6. TERMINATION 5
- 7. REQUEST FOR WAIVER AND WAIVER OF BREACH 6
- 8. TRANSITION PERIOD 6
- 9. OWNERSHIP, PUBLICATION, REPRODUCTION, AND USE OF MATERIAL 6
- 10. CONDUCT OF CONTRACTOR/ CONFLICT OF INTEREST 6
- 11. REPLACEMENT PRODUCTS 7
- 12. RECORDS, INSPECTIONS, AND AUDITS 7
- 13. CONFIDENTIALITY 8
- 14. HEALTH INSURANCE PORTABILITY ACCOUNTABILITY ACT 8
- 15. MEDI-CAL PERSONALLY IDENTIFIABLE INFORMATION 8
- 16. PERSONALLY IDENTIFIABLE INFORMATION 9
- 17. HOLD HARMLESS/INDEMNIFICATION 9
- 18. INSURANCE 10
- 19. WORKER'S COMPENSATION 11
- 20. VEHICLE LIABILITY 11
- 21. COMMERCIAL GENERAL LIABILITY 11
- 22. PROFESSIONAL LIABILITY 12
- 23. CYBER LIABILITY 12
- 24. INDEPENDENT CONTRACTOR 12
- 25. USE BY POLITICAL ENTITIES 13
- 26. LICENSES AND PERMITS 13
- 27. NO DEBARMENT OR SUSPENSION 13
- 28. COMPLIANCE WITH RULES, REGULATIONS, AND DIRECTIVES 13
- 29. EMPLOYMENT PRACTICES 13
- 30. LOBBYING 14
- 31. ADVERSE GOVERNMENT ACTION 14
- 32. SUBCONTRACTS 14
- 33. SUPPLANTATION 15
- 34. ASSIGNMENT 15
- 35. FORCE MAJEURE 15
- 36. GOVERNING LAW 15
- 37. DISPUTES 16
- 38. ADMINISTRATIVE/CONTRACT LIAISON 16
- 39. NOTICES 16
- 40. SIGNED IN COUNTERPARTS 16
- 41. ELECTRONIC SIGNATURES 17
- 42. MODIFICATION OF TERMS 17
- 43. ENTIRE AGREEMENT 17

List of Schedules
 Schedule A – Payment Provisions
 Schedule B – Scope of Services

List of Attachments

Attachment I – DPSS 2076A, DPSS 2076B & Instructions

Attachment II – PII Privacy and Security Standards

Attachment III – Medi-Cal Privacy & Security Agreement

Attachment IV – HIPAA Business Associate Agreement

This Professional Services Agreement for software management services is made and entered into this ____ day of _____, 2021, by and between JUMP Technology Services, L.L.C., an Oklahoma limited liability company (herein referred to as "CONTRACTOR"), and the County of Riverside, a political subdivision of the State of California, on behalf of its Department of Public Social Services (herein referred to as "COUNTY"). The parties agree as follows:

1. DEFINITIONS

- A. "CONTRACTOR" refers to JUMP Technology Services, L.L.C. and its employees, agents and representatives providing services under this Agreement.
- B. "DPSS and/or COUNTY" refers to the COUNTY of Riverside and its Department of Public Social Services, which has administrative responsibility for this Agreement.
- C. "Help Desk Ticket (HDT)" shall mean a problem identified by unique number in CONTRACTOR's Help Desk system.
- D. "Enhancement" shall mean any modification or addition that, when made or added to a software system, materially changes its utility, efficiency, functional capability, but that does not constitute solely an Error Correction. Enhancements may be designated by CONTRACTOR as minor or major, depending on CONTRACTOR's assessment of their value and of the function added to the software system.
- E. "Error" shall mean any failure of the software system to conform in all material responses to its functional specifications as documented in the software system manuals or scope of work.
- F. "Error correction" shall mean either a modification or an addition that, when made or added to a software system, establishes material conformity of the software system to the functional specifications or a procedure or routine that, when observed in the regular operation of the software system, eliminates the practical adverse effect on COUNTY of such nonconformity.
- G. "Maintenance Services" shall mean the services provided under CONTRACTOR's Maintenance and Support Services policy as detailed in Schedule B, Scope of Services.
- H. "Major Release" shall mean a new version of the software system that includes Enhancements, upgrade in features, functionality or performance of the software system.
- I. "Software System" shall mean the software system(s) licensed to COUNTY by CONTRACTOR as identified in the License Agreement or owned by the COUNTY in the event CONTRACTOR is contracting for support services of a software system CONTRACTOR does not own.
- J. "Subcontract" refers to any contract, purchase order, or other purchase agreement, including modifications and change orders to the foregoing, entered into by the Contractor with a subcontractor to furnish supplies, materials, equipment, and services for the performance of any of the terms and conditions contained in this Agreement.
- K. "Subcontractor" means any supplier, vendor, or firm that furnishes supplies, materials, equipment, or services to or for the Contractor or another subcontractor.

L. "Updates" shall mean subsequent releases of the Major Release that provide minor Enhancements or Error Corrections. Updates are made available at no charge to software systems receiving Maintenance Service.

2. DESCRIPTION OF SERVICES

CONTRACTOR shall provide all services at the prices stated in Schedule A, Payment Provisions, and as outlined and specified in Schedule B, Scope of Services, and Attachment I DPSS 2076A, DPSS 2076B & Instructions, Attachment II PII Privacy and Security Standards, Attachment III Medi-Cal Privacy & Security Agreement, and Attachment IV HIPAA Business Associate Agreement.

3. PERIOD OF PERFORMANCE

This Agreement shall be effective July 1, 2021 and continue through June 30, 2026, unless terminated earlier. CONTRACTOR shall commence performance upon the effective date and shall diligently and continuously perform thereafter.

4. COMPENSATION

COUNTY shall pay CONTRACTOR for services performed, products provided, or expenses incurred in accordance with Schedule A, "Payment Provisions. COUNTY is not responsible for any fees or costs incurred above or beyond the contracted amount and shall have no obligation to purchase any specified amount of services or product. Unless otherwise specifically stated in Schedule A, COUNTY shall not be responsible for payment of any of CONTRACTOR's expenses related to this Agreement. At the expiration of the term of this Agreement, or upon termination prior to the expiration of the Agreement, any funds paid to CONTRACTOR, but not used for purposes of this Agreement shall revert to COUNTY within thirty (30) calendar days of the expiration or termination.

5. AVAILABILITY OF FUNDS/NON-APPROPRIATION OF FUNDS

The obligation of COUNTY for payment under this Agreement beyond the current fiscal year is contingent upon and limited by the availability of county funding from which payment can be made. There shall be no legal liability for payment on the part of COUNTY beyond June 30 of each year unless funds are made available for such payment by the County Board of Supervisors. In the event such funds are not forthcoming for any reason, COUNTY shall immediately notify CONTRACTOR in writing and this Agreement shall be deemed terminated and be of no further force or effect. COUNTY shall make all payments to CONTRACTOR that were properly earned prior to the unavailability of funding.

6. TERMINATION

A. COUNTY may terminate this Agreement without cause upon giving thirty (30) calendar days written notice served on CONTRACTOR stating the extent and effective date of termination.

B. COUNTY may, upon five (5) calendar days written notice, terminate this Agreement for CONTRACTOR's default, if CONTRACTOR refuses or fails to comply with the terms of this Agreement, or fails to make progress that may endanger performance and does not immediately cure such failure. In the event of such termination, COUNTY may proceed with the work in any manner deemed proper by COUNTY.

C. After receipt of the notice of termination, CONTRACTOR shall:

(1) Stop all work under this Agreement on the date specified in the notice of termination; and

- (2) Transfer to COUNTY and deliver in the manner directed by COUNTY any materials, reports or other products, which, if the Agreement had been completed or continued, would be required to be furnished to COUNTY.
 - D. After termination, COUNTY shall make payment only for CONTRACTOR's performance up to the date of termination in accordance with this Agreement.
 - E. CONTRACTOR's rights under this Agreement shall terminate (except for fees accrued prior to the date of termination) upon dishonestly or willful and material breach of this Agreement by CONTRACTOR; or in the event of CONTRACTOR's unwillingness or inability, for any reason whatsoever, to perform the terms of this Agreement. In such an event, CONTRACTOR shall not be entitled to any further compensation under this Agreement.
 - F. The rights and remedies of COUNTY provided in this section shall not be exclusive and are in addition to any other rights or remedies provided by law or this Agreement.
7. **REQUEST FOR WAIVER AND WAIVER OF BREACH**
 Waiver of any provision of this Agreement must be in writing and signed by authorized representatives of the parties. No waiver or breach of any provision of the terms and conditions herein shall be deemed, for any purpose, to be a waiver or a breach of any other provision hereof, or of a continuing or subsequent waiver or breach. Failure of COUNTY to require exact, full compliance with any terms of this Agreement shall not be construed as making any changes to the terms of this Agreement and does not prevent COUNTY from enforcing the terms of this Agreement.
8. **TRANSITION PERIOD**
 CONTRACTOR recognizes that the services under this Agreement are vital to COUNTY and must be continued without interruption and that, upon expiration, COUNTY or another contractor may continue the services outlined herein. CONTRACTOR agrees to exercise its best efforts and cooperation to affect an orderly and efficient transition of clients or services to a successor.
9. **OWNERSHIP, PUBLICATION, REPRODUCTION, AND USE OF MATERIAL**
 JUMP retains sole rights to the intellectual property of all work products. JUMP will grant COUNTY unlimited license to use the product with the exception of those work items that are included in our compiled software delivered as a service.
10. **CONDUCT OF CONTRACTOR/ CONFLICT OF INTEREST**
- A. CONTRACTOR covenants that it presently has no interest, including but not limited to, other projects or contract, and shall not acquire any such interest, direct or indirect, which would conflict in any manner or degree with CONTRACTOR's performance under this Agreement. CONTRACTOR further covenants that no person or subcontractor having any such interest shall be employed or retained by CONTRACTOR under this Agreement. CONTRACTOR agrees to inform the COUNTY of all CONTRACTOR's interest, if any, which are or may be perceived as incompatible with COUNTY's interests.
 - B. CONTRACTOR shall not, under any circumstances which could be perceived as to influence the recipient in the conduct of his/her duties, accept any gratuity or special favor from individuals or firms with whom CONTRACTOR is doing business or proposing to do business, in fulfilling this Agreement.

11. REPLACEMENT PRODUCTS

1. If the CONTRACTOR, within four years from the last agreement date between the COUNTY and the CONTRACTOR for the Software, generally or commercially releases a product (hereinafter "Replacement Product(s)") with the same or substantially similar functionality as that of the Software licensed by COUNTY pursuant to such agreement, and the CONTRACTOR concurrently or within one (1) year from such release date discontinues the support of the most recent generally released version of the Software, then the COUNTY shall receive a credit for the full value of the License fees paid by COUNTY for the Software toward the purchase of the Replacement Product, provided that COUNTY is a subscriber to the Maintenance and Support Services for the Software. The Replacement Product shall be treated as Software for the purpose of this Agreement.
2. The License granted to the COUNTY for the Replacement Product shall be:
 - a. pursuant to the terms and conditions of this Agreement,
 - b. granted without the payment of additional fees; and
 - c. the COUNTY's Maintenance and Support fees for the Replacement Product shall remain the same as for the Licensed Product for the remainder of the support term.

12. RECORDS, INSPECTIONS, AND AUDITS

- A. All performance, including services, workmanship, materials, facilities or equipment utilized in the performance of this Agreement, shall be subject to inspection and test by COUNTY or any other regulatory agencies at all times. This may include, but is not limited to, monitoring or inspecting contractor performance through any combination of on-site visits, inspections, evaluations, and CONTRACTOR self-monitoring. CONTRACTOR shall cooperate with any inspector or COUNTY representative reviewing compliance with this Agreement and permit access to all necessary locations, equipment, materials, or other requested items.
- B. CONTRACTOR shall maintain auditable books, records, documents, and other evidence relating to costs and expenses to this Agreement. CONTRACTOR shall maintain these records for at least three (3) years after final payment has been made or until pending county, state, and federal audits are completed, whichever is later.
- C. Any authorized county, state or the federal representative shall have access to all books, documents, papers, electronic data and other records they determine are necessary to perform an audit, evaluation, inspection, review, assessment, or examination. These representatives are authorized to obtain excerpts, transcripts and copies as they deem necessary and shall have the same right to monitor or inspect the work or services as COUNTY.
- D. If CONTRACTOR disagrees with an audit, CONTRACTOR may employ a Certified Public Accountant (CPA) to prepare and file with COUNTY its own certified financial and compliance audit. CONTRACTOR shall not be reimbursed by COUNTY for such an audit regardless of the audit outcome.
- E. CONTRACTOR shall establish sufficient procedures to self-monitor the quality of services/products under this Agreement and shall permit COUNTY or other inspector to assess and evaluate CONTRACTOR's performance at any time, upon reasonable notice to the CONTRACTOR.

13. CONFIDENTIALITY

- A. As required by applicable law, COUNTY and CONTRACTOR shall maintain the privacy and confidentiality of all information and records, regardless of format, received pursuant to the Agreement ("confidential information"). Confidential information includes, but is not limited to, unpublished or sensitive technological or scientific information; medical, personnel, or security records; material requirements or pricing/purchasing actions; COUNTY information or data which is not subject to public disclosure; COUNTY operational procedures; and knowledge of contractors, subcontractors or suppliers in advance of official announcement. CONTRACTOR shall ensure that no person will publish, disclose, use or cause to be disclosed such confidential information pertaining to any applicant or recipient of services. CONTRACTOR shall keep all confidential information received from COUNTY in the strictest confidence. CONTRACTOR shall comply with Welfare and Institutions Code Section 10850.
- B. CONTRACTOR shall take special precautions, including but not limited to, sufficient training of CONTRACTOR's staff before they begin work, to protect such confidential information from loss or unauthorized use, access, disclosure, modification or destruction.
- C. CONTRACTOR shall ensure case record or personal information is kept confidential when it identifies an individual by name, address, or other specific information. CONTRACTOR shall not use such information for any purpose other than carrying out CONTRACTOR's obligations under this Agreement.
- D. CONTRACTOR shall promptly transmit to COUNTY all third-party requests for disclosure of confidential information. CONTRACTOR shall not disclose such information to anyone other than COUNTY except when disclosure is specifically permitted by this Agreement or as authorized in writing in advance by COUNTY.
- E. Each Party shall immediately notify the other when it discovers that there may have been a breach in security which has or may have resulted in compromise to confidential data. For purposes of this section, immediately is defined as within two hours of discovery.

The County contact for such notification is as follows:

DPSS Privacy and Security Officer
 Riverside County Department of Public Social Services
 7894 Mission Grove Parkway, Suite 100
 Riverside, CA 92508
 (951) 358-6841

14. HEALTH INSURANCE PORTABILITY ACCOUNTABILITY ACT

CONTRACTOR is subject to and shall operate in compliance with all relevant requirements contained in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, enacted August 21, 1996, and the related laws and regulations promulgated subsequent thereto. The parties agree to the terms and conditions of the HIPAA Business Associate Agreement attached as Attachment IV.

15. MEDI-CAL PERSONALLY IDENTIFIABLE INFORMATION

"Medi-Cal PII" refers to Medi-Cal Personally Identifiable Information which is directly obtained in the course of performing an administrative function on behalf of Medi-Cal, such as determining Medi-Cal eligibility or conducting In Home Supportive Services (IHSS) operations, that can be used alone, or in conjunction with any other information, to identify a specific individual. PII

includes any information that can be used to search for or identify individuals, or can be used to access their files, such as name, social security number, date of birth, driver's license number or identification number. PII may be electronic or paper.

The CONTRACTOR may use or disclose Medi-Cal Personally Identifiable Information (PII) only to perform functions, activities or services directly related to the administration of the Medi-Cal program in accordance with Welfare and Institutions Code section 14100.2 and 42 Code of Federal Regulations section 431.300 et.seq, or as required by law. Disclosures which are required by law, such as a court order, or which are made with the explicit written authorization of the Medi-Cal client, are allowable. Any other use or disclosure of Medi-Cal PII requires the express approval in writing of the COUNTY. The CONTRACTOR shall not duplicate, disseminate or disclose Medi-Cal PII except as allowed in this Agreement.

The CONTRACTOR agrees to the same privacy and security safeguards as are contained in the Medi-Cal Data Privacy and Security Agreement, attached hereto and incorporated by this reference as Attachment III.

When applicable, the CONTRACTOR shall incorporate the relevant provisions of Attachment III into each subcontract or sub-award to subcontractors.

16. PERSONALLY IDENTIFIABLE INFORMATION

- A. Personally Identifiable Information (PII) refers to personally identifiable information that can be used alone or in conjunction with any other reasonably available information, to identify a specific individual. 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. PII may be collected through 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. CONTRACTOR may use or disclose PII only to perform functions, activities or services directly related to the administration of programs in accordance with Welfare and Institutions Code sections 10850 and 14100.2, or 42 Code of Federal Regulations (CFR) section 431.300 et.seq, and 45 CFR 205.50 et.seq, or as required by law. Disclosures which are required by law, such as a court order, or which are made with the explicit written authorization of the client, are allowable. Any other use or disclosure requires the express approval in writing of the COUNTY. CONTRACTOR shall not duplicate, disseminate or disclose PII except as allowed in this Agreement.
- C. CONTRACTOR agrees to the PII Privacy and Security Standards attached as Attachment II. When applicable, CONTRACTOR shall incorporate the relevant provisions of Attachment II into each subcontract or sub-award to subcontractors.

17. HOLD HARMLESS/INDEMNIFICATION

CONTRACTOR agrees to indemnify and hold harmless COUNTY, its departments, agencies and districts, including their respective officers, Board of Supervisors, elected and appointed officials, employees, agents and representatives (collectively "County Indemnitees"), from any liability, damage, claim or action based upon or related to any services or work of CONTRACTOR (including its officers, employees, agents, subcontractors or suppliers) arising out of or in any way relating to this Agreement, including but not limited to property damage, bodily injury or death. CONTRACTOR shall, at its sole expense and cost including but not limited to, attorney fees, cost

of investigation, defense, and settlements or awards, defend County Indemnitees in any such claim or action. CONTRACTOR shall, at their sole cost, have the right to use counsel of their choice, subject to the approval of COUNTY which shall not be unreasonably withheld; and shall have the right to adjust, settle, or compromise any such claim or action so long as that does not compromise CONTRACTOR's indemnification obligation. CONTRACTOR's obligation hereunder shall be satisfied when CONTRACTOR has provided COUNTY the appropriate form of dismissal relieving COUNTY from any liability for the action or claim made. The insurance requirements stated in this Agreement shall in no way limit or circumscribe CONTRACTOR's obligations to indemnify and hold COUNTY harmless.

18. INSURANCE

- A. Without limiting or diminishing CONTRACTOR's obligation to indemnify or hold COUNTY harmless, CONTRACTOR shall procure and maintain or cause to be maintained, at its sole cost and expense, the following insurance coverages during the term of this Agreement. As respects to the insurance section only, COUNTY herein refers to the County of Riverside, its agencies, districts, special districts, and departments, their respective directors, officers, Board of Supervisors, employees, elected or appointed officials, agents, or representatives as Additional Insureds.
- B. Any insurance carrier providing insurance coverage hereunder shall be admitted to the State of California and have an AM BEST rating of not less than A: VIII (A:8) unless such requirements are waived, in writing, by the County Risk Manager. If the County's Risk Manager waives a requirement for a particular insurer such waiver is only valid for that specific insurer and only for one policy term.
- C. CONTRACTOR's insurance carrier(s) must declare its insurance self-insured retentions. If such self-insured retentions exceed \$500,000 per occurrence such retentions shall have the prior written consent of the County Risk Manager before the commencement of operations under this Agreement. Upon notification of self-insured retention unacceptable to COUNTY, and at the election of the County's Risk Manager, CONTRACTOR's carriers shall either; 1) reduce or eliminate such self-insured retention as respects to this Agreement with COUNTY, or 2) procure a bond which guarantees payment of losses and related investigations, claims administration, and defense costs and expenses.
- D. CONTRACTOR shall cause CONTRACTOR's insurance carrier(s) to furnish the COUNTY with either 1) a properly executed original certificate(s) of insurance and certified original copies of endorsements effecting coverage as required herein, or 2) if requested to do so orally or in writing by the County Risk Manager, provide original certified copies of policies, including all endorsements and all attachments thereto, showing such insurance is in full force and effect. Further, said Certificate(s) and policies of insurance shall contain the covenant of the insurance carrier(s) that thirty (30) calendar days written notice shall be given to the COUNTY prior to any material modification, cancellation, expiration or reduction in coverage of such insurance. In the event of a material modification, cancellation, expiration, or reduction in coverage, this Agreement shall terminate forthwith, unless the COUNTY receives, prior to such effective date, another properly executed original Certificate of Insurance and original copies of endorsements or certified original policies, including all endorsements and attachments thereto evidencing coverages set forth herein and the insurance required herein is in full force and effect. CONTRACTOR shall not commence operations until the COUNTY has been furnished original certificate(s) of insurance and certified original copies of endorsements and if requested, certified original policies of insurance including all endorsements and any and all other attachments as required in this section. An individual

authorized by the insurance carrier to do so on its behalf shall sign the original endorsements for each policy and the certificate of insurance.

- E. It is understood and agreed to by the parties hereto that CONTRACTOR's insurance shall be construed as primary insurance, and COUNTY's insurance and/or deductibles and/or self-insured retentions or self-insured programs shall not be construed as contributory.
- F. If, during the term of this Agreement or any extension thereof, there is a material change in the scope of services, or there is a material change in the equipment to be used in the performance of the scope of work which will add additional exposures (such as the use of aircraft, watercraft, cranes, etc.), or the term of this Agreement, including any extensions thereof, exceeds five (5) years, the COUNTY reserves the right to adjust the types of insurance required under this Agreement and the monetary limits of liability for the insurance coverages currently required herein if, in the County Risk Manager's reasonable judgment, the amount or type of insurance carried by the CONTRACTOR has become inadequate.
- G. CONTRACTOR shall pass down the insurance obligations contained herein to all tiers of subcontractors working under this Agreement.
- H. The insurance requirements contained in this Agreement may be met with a program(s) of self-insurance acceptable to COUNTY.
- I. CONTRACTOR agrees to notify COUNTY of any claim by a third party or any incident or event that may give rise to a claim arising from the performance of this Agreement.

19. WORKER'S COMPENSATION

If CONTRACTOR has employees as defined by the State of California, CONTRACTOR shall maintain statutory Worker's Compensation Insurance (Coverage A) as prescribed by the laws of the State of California. Policy shall include Employers' Liability (Coverage B) including Occupational Disease with limits not less than \$1,000,000 per person per accident. The policy shall be endorsed to waive subrogation in favor of the County of Riverside.

20. VEHICLE LIABILITY

If vehicles or mobile equipment are used in the performance of the obligations under this Agreement, then CONTRACTOR shall maintain liability insurance for all owned, non-owned or hired vehicles so used in an amount not less than \$1,000,000 per occurrence combined single limit. If such insurance contains a general aggregate limit, it shall apply separately to this Agreement or be no less than two (2) times the occurrence limit. Policy shall name COUNTY as additional Insured.

21. COMMERCIAL GENERAL LIABILITY

Commercial General Liability insurance coverage, including but not limited to, premises liability, contractual liability, products and completed operations liability, personal and advertising injury, and cross liability coverage, covering claims which may arise from or out of CONTRACTOR's performance of its obligations hereunder. Policy shall name the COUNTY as additional Insured. Policy's limit of liability shall not be less than \$1,000,000 per occurrence combined single limit. If such insurance contains a general aggregate limit, it shall apply separately to this Agreement or be no less than two (2) times the occurrence limit.

22. PROFESSIONAL LIABILITY

If, at any time during the duration of this Agreement and any renewal or extension thereof, the CONTRACTOR, its employees, agents or subcontractors provide professional counseling for issues of medical diagnosis, medical treatment, mental health, dispute resolution or any other services for which it is the usual and customary practice to maintain Professional Liability Insurance, the CONTRACTOR shall procure and maintain Professional Liability Insurance (Errors & Omissions), providing coverage for performance of work included within this Agreement, with a limit of liability of not less than \$1,000,000 per occurrence and \$2,000,000 annual aggregate. If CONTRACTOR's Professional Liability Insurance is written on a claim made basis rather than an occurrence basis, such insurance shall continue through the term of this Agreement. Upon termination of this Agreement or the expiration or cancellation of the claims made insurance policy CONTRACTOR shall purchase at his sole expense either 1) an Extended Reporting Endorsement (also known as Tail Coverage); or, 2) Prior Dates Coverage from a new insurer with a retroactive date back to the date of, or prior to, the inception of this Agreement; or, 3) demonstrate through Certificates of Insurance that CONTRACTOR has maintained continuous coverage with the same or original insurer. Coverage provided under items 1), 2) or 3) will continue for a period of five (5) years beyond the termination of this Agreement.

23. CYBER LIABILITY

CONTRACTOR shall procure and maintain for the duration of the contract insurance against claims for injuries to person or damages to property which may arise from or in connection with the performance of the work hereunder by CONTRACTOR, its agents, representatives, or employees. CONTRACTOR shall procure and maintain for the duration of the contract insurance claims arising out of their services and including, but not limited to loss, damage, theft or other misuse of data, infringement of intellectual property, invasion of privacy and breach of data.

CONTRACTOR shall procure and maintain cyber liability Insurance, with limits not less than \$2,000,000 per occurrence or claim, \$2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by CONTRACTOR in this Agreement and shall include, but not limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

If CONTRACTOR maintains broader coverage and/or higher limits than the minimums shown above, COUNTY requires and shall be entitled to the broader coverage and/or higher limits maintained by CONTRACTOR. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to COUNTY.

24. INDEPENDENT CONTRACTOR

It is agreed that CONTRACTOR is an independent contractor and that no relationship of employer-employee exists between the parties. CONTRACTOR and its employees shall not be entitled to any benefits payable to employees of COUNTY, including but not limited to, workers' compensation, retirement, or health benefits. COUNTY shall not be required to make any deductions for CONTRACTOR employees from the compensation payable to CONTRACTOR under this Agreement. CONTRACTOR agrees to hold COUNTY harmless from any and all claims that may be made against COUNTY based upon any contention by any person or other party that an employer-employee relationship exists by reason of this Agreement. CONTRACTOR agrees to indemnify and defend, at its sole expense and cost, including but not limited, to attorney fees,

cost of investigation, defense and settlements, or awards, COUNTY, its officers, agents, and employees in any legal action based upon such alleged existence of an employer-employee relationship by reason of this Agreement.

25. USE BY POLITICAL ENTITIES

CONTRACTOR agrees to extend the same pricing, terms, and conditions as stated in this Agreement to each and every political entity, special district, and related non-profit entity in Riverside County, and to every political entity located in the State of California. It is understood that other entities shall make purchases in their own name, make direct payment, and be liable directly to CONTRACTOR; and COUNTY shall in no way be responsible to CONTRACTOR for other entities' purchases.

26. LICENSES AND PERMITS

If applicable, CONTRACTOR shall be licensed and have all permits as required by Federal, State, County, or other regulatory authorities at the time the proposal is submitted to COUNTY and throughout the term of this Agreement. CONTRACTOR warrants that it has all necessary permits, approvals, certificates, waivers, and exceptions necessary for performance of this Agreement.

27. NO DEBARMENT OR SUSPENSION

CONTRACTOR certifies that it is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by a federal department or agency; has not within a three-year period preceding this Agreement been convicted of or had a civil judgment rendered against it for the commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state or local) transaction; violation of federal or state anti-trust status; commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property; is not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state or local) with commission of any of the offenses enumerated herein; and has not within a three-year period preceding this Agreement had one or more public transactions (federal, state or local) terminated for cause or default.

28. COMPLIANCE WITH RULES, REGULATIONS, AND DIRECTIVES

CONTRACTOR shall comply with all rules, regulations, requirements and directives of the California Department of Social Services, other applicable State or Federal agencies, funding sources and other governing regulatory authorities which impose duties and regulations upon COUNTY related to this Agreement. These shall be equally applicable to and binding upon CONTRACTOR to the same extent as they are upon COUNTY.

29. EMPLOYMENT PRACTICES

A. CONTRACTOR shall comply with all federal and state statutes and regulations in the hiring of its employees.

B. CONTRACTOR shall not discriminate in its recruiting, hiring, promoting, demoting, or terminating practices on the basis of race, religious creed, color, national origin, ancestry, physical handicap, medical condition, marital status, age, or sex in the performance of this Agreement; if applicable, with the provisions of the Fair Employment and Housing Act (FEHA) and the Federal Civil Rights Act of 1964 (P. L. 88-352).

C. In the provision of benefits, CONTRACTOR shall certify and comply with Public Contract Code 10295.3 and not discriminate between employees with spouses and employees with domestic partners or discriminate between the domestic partners and spouses of those employees. For

the purpose of this section "domestic partner" means one of two persons who have filed a declaration of domestic partnership with the Secretary of State pursuant to Division 2.5 (commencing with Section 297) of the Family Code.

- D. By signing this Agreement or accepting funds under this Agreement, CONTRACTOR shall comply with Executive Order 11246 of September 24, 1965, entitled "Equal Employment Opportunity," as amended by Department of Labor regulations (41 CFR Chapter 60).
- E. Employment Development Department reporting requirements: CONTRACTOR shall provide required data and certification to COUNTY in order to comply with child support enforcement requirements. The documentation will be provided within ten (10) days of notification of award of this Agreement when required by the Employment Development Department. Failure to submit the documentation or failure to comply with all federal and state reporting requirements for child support enforcement shall constitute a material breach of this Agreement.

30. LOBBYING

- A. CONTRACTOR shall ensure no federal appropriated funds have been paid or will be paid by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the awarding of any federal contract, continuation, renewal, amendment, or modification of any federal contract, grant loan or cooperative agreement.
- B. If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with such federal contract, grant, loan, or cooperative agreement, CONTRACTOR shall complete and submit Standard Form LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.
- C. CONTRACTOR shall require that the language of this certification be included in the award document for sub-awards at all tiers, including subcontracts, sub-grants, and contract under grants, loans, and cooperative agreements, and that all sub-recipients shall certify and disclose accordingly.

31. ADVERSE GOVERNMENT ACTION

In the event any action of any department, branch or bureau of the federal, state, or local government has a material adverse effect on either party in the performance of their obligations hereunder, then that party shall notify the other of the nature of this action, including in the notice a copy of the adverse action. The parties shall meet within thirty (30) calendar days and shall, in good faith, attempt to negotiate a modification to this Agreement that minimizes the adverse effect. Notwithstanding the provisions herein, if the parties fail to reach a negotiated modification concerning the adverse action, then the affected party may terminate this Agreement by giving at least one hundred eighty (180) calendar days' notice or may terminate sooner if agreed to by both parties.

32. SUBCONTRACTS

- A. CONTRACTOR shall not enter into any subcontract with any subcontractor who:
 - (1) Is presently debarred, suspended, proposed for debarment or suspension, or declared ineligible or voluntarily excluded from covered transactions by a federal department or agency;

- (2) Has within a three-year period preceding this Agreement been convicted of or had a civil judgment rendered against them for the commission of fraud, a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state or local) transaction, violation of federal or state anti-trust status, commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
- (3) Is presently indicted or otherwise criminally or civilly charged by a government entity (federal, state or local) with commission of any of the offenses enumerated in the paragraph above; and
- (4) Has within a three-year period preceding this Agreement had one or more public transactions (federal, state or local) terminated for cause or default.

- B. CONTRACTOR shall be fully responsible for the acts or omissions of its subcontractors and the subcontractors' employees.
- C. CONTRACTOR shall insert clauses in all subcontracts to bind its subcontractors to the terms and conditions of this Agreement.
- D. Nothing contained in this Agreement shall create a contractual relationship between any subcontractor or supplier of CONTRACTOR and COUNTY.

33. SUPPLANTATION

CONTRACTOR shall not supplant any federal, state or county funds intended for the purpose of this Agreement with any funds made available under any other agreement. CONTRACTOR shall not claim reimbursement from COUNTY for any sums which have been paid by another source of revenue. CONTRACTOR agrees that it will not use funds received pursuant to this Agreement, either directly or indirectly, as a contribution or compensation for purposes of obtaining state funds under any state program or COUNTY funds under any county programs without prior approval of COUNTY.

34. ASSIGNMENT

CONTRACTOR shall not assign or transfer any interest in this Agreement without the prior written consent of COUNTY. Any attempt to assign or transfer any interest without written consent of COUNTY shall be deemed void and of no force or effect.

35. FORCE MAJEURE

If either party is unable to comply with any provision of this Agreement due to causes beyond its reasonable control and which could not have been reasonably anticipated, such as acts of God, acts of war, civil disorders, or other similar acts, such party shall not be held liable for such failure to comply.

36. GOVERNING LAW

This Agreement shall be governed by the laws of the State of California. Any legal action related to the interpretation or performance of this Agreement shall be filed only in the Superior Court for the State of California or the U.S. District Court located in Riverside, California.

37. DISPUTES

- A. The parties shall attempt to resolve any disputes amicably at the working level. If that is not successful, the dispute shall be referred to the senior management of the parties. Any dispute relating to this Agreement which is not resolved by the parties shall be decided by COUNTY's Compliance Contract Officer who shall furnish the decision in writing. The decision of COUNTY's Compliance Contract Officer shall be final and conclusive unless determined by a court to have been fraudulent, capricious, arbitrary, or so grossly erroneous as necessarily to imply bad faith. CONTRACTOR shall proceed diligently with the performance of this Agreement pending resolution of a dispute.
- B. Prior to the filing of any legal action related to this Agreement, the parties shall be obligated to attend a mediation session in Riverside County before a neutral third-party mediator. A second mediation session shall be required if the first session is not successful. The parties shall share the cost of the mediations.

38. ADMINISTRATIVE/CONTRACT LIAISON

Each party shall designate a liaison that will be the primary point of contact regarding this Agreement.

39. NOTICES

All notices, claims, correspondence, or statements authorized or required by this Agreement shall be deemed effective three (3) business days after they are made in writing and deposited in the United States mail addressed as follows:

COUNTY:

Department of Public Social Services
Contracts Administration Unit
P.O. Box 7789
Riverside, CA 92513

Invoices and other financial documents:

Department of Public Social Services
Fiscal/Management Reporting Unit
4060 County Circle Drive
Riverside, CA 92503

CONTRACTOR:

JUMP Technology Services, L.L.C.
1024 Iron Point Road
Folsom, CA 95630

CONTRACTOR "Remit To" address:

JUMP Technology Services, L.L.C.
P.O. Box 3452
Edmond, OK 73083

40. SIGNED IN COUNTERPARTS

This agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all counterparts together shall constitute a single agreement.

- 41. **ELECTRONIC SIGNATURES**
Each party of this MOU agrees to the use of electronic signatures, such as digital signatures that meet the requirements of the California Uniform Electronic Transactions Act ("CUETA") Cal. Civ. Code §§ 1633.1 to 1633.17), for executing this MOU. The parties further agree that the electronic signature(s) included herein are intended to authenticate this writing and to have the same force and effect as manual signatures. Electronic signature means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record pursuant to the CUETA as amended from time to time. Digital signature means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature, and shall be reasonably relied upon by the parties. For purposes of this section, a digital signature is a type of "electronic signature" as defined in subdivision (i) of Section 1633.2 of the Civil Code.
- 42. **MODIFICATION OF TERMS**
This Agreement may be modified only by a written amendment signed by authorized representatives of both parties. Requests to modify fiscal provisions shall be submitted no later than April 1.
- 43. **ENTIRE AGREEMENT**
This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. All prior or contemporaneous agreements of any kind or nature relating to the same subject matter shall be of no force or effect.

Authorized Signature for JUMP Technology Services, L.L.C.: 	Authorized Signature for County of Riverside: 
Printed Name of Person Signing: Denise Brinkmeyer	Printed Name of Person Signing: Karen Spiegel
Title: President	Title: Chair, Board of Supervisors
Date Signed: Jan 28, 2021	Date Signed: 

ATTEST:
 KECIA R. HARPER, Clerk
 By  DEPUTY

FORM APPROVED COUNTY COUNSEL
 BY  2.3.2021
 SYNTHIA M. GUNZEL DATE

Schedule A
Payment Provisions

A.1 MAXIMUM AMOUNTS –ANNUAL AND AGGREGATE TOTALS

The total payments by COUNTY to CONTRACTOR shall not exceed \$168,000 annually, including all expenses. Funds may be shifted between the Software License and Maintenance and Support category provided that the maximum aggregate amount of the contract is not exceeded. Advance approval from DPSS is required for reallocating funds.

FISCAL YEAR PERIOD	SOFTWARE LICENSE <i>(Level 300-350)</i>	ENHANCEMENTS/ MAINTENANCE & SUPPORT <i>(outside of standard maintenance set forth in Schedule B, Section B.3)</i>	ANNUAL TOTAL
July 1, 2021 through June 30, 2022	\$150,500	\$17,500	\$168,000
July 1, 2022 through June 30, 2023	\$150,500	\$17,500	\$168,000
July 1, 2023 through June 30, 2024	\$150,500	\$17,500	\$168,000
July 1, 2024 through June 30, 2025	\$150,500	\$17,500	\$168,000
July 1, 2025 through June 30, 2026	\$150,500	\$17,500	\$168,000
Maximum reimbursable amount:	\$757,500	\$87,500	\$840,000

A.2 The COUNTY is not responsible for any fees or costs incurred above or beyond the contracted amount and shall have no obligation to purchase any specified amount of services or products. Unless otherwise specifically stated in Schedule A, COUNTY shall not be responsible for payment of any of CONTRACTOR's expenses related to this Agreement.

A.3 The COUNTY will utilize the CONTRACTORS 300 to 350 license user level annually. The COUNTY will not be able to add additional accounts without inactivating active licenses, not to exceed the license limit referenced in this Agreement. The COUNTY may request a quotation for the next license level which will be quoted not to exceed the per license cost of the current level.

A.4 METHOD, TIME, AND CONDITIONS OF PAYMENT

- a. CONTRACTOR will be paid the actual amount of each approved monthly invoice. COUNTY may delay payment if the required supporting documentation is not provided or other requirements are not met.
 - 1. DPSS Forms 2076A, following the instructions set forth. Attachment I is attached hereto and incorporated herein by this reference for all payment requests.
 - 2. Project Estimates approved by DPSS. Project Estimate will include a statement of work, deliverables, project timeline, and cost.
- b. All payment claims shall be submitted on a monthly basis no later than 30 days after the end of each month in which the services were provided. Each payment claiming period shall consist of a calendar month. All complete claims submitted in a timely manner shall be processed within forty-five (45) calendar days.

- d. CONTRACTOR invoice estimates for May and June are due no later than June 5. Actual CONTRACTOR invoices for May and June are due no later than July 30.

A.5 INVOICES

Invoices will include in instances where software is electronically delivered the following language: "All products purchased are available via electronic download only. No tangible media or documentation will be available or shipped. Access to the products purchased and referenced on this invoice is in no way dependent upon any tangible media that may have been received prior to or separately from this purchase."

Each invoice shall contain a minimum of the following information: invoice number and date; remittance address; bill-to and ship-to addresses of ordering department/division; Agreement number (DPSS-0002444); quantities; item descriptions, unit prices, extensions, sales/use tax if applicable, and an invoice total.

A.6 SALES AND USE TAX

Fees set forth herein shall include applicable California and other state and local sales/use taxes on all Software products procured by COUNTY pursuant to or otherwise due as a result of this Agreement. All California sales/use taxes shall be paid directly by CONTRACTOR to the State or other taxing authority. CONTRACTOR shall be solely liable and responsible for payment of any and all California and other state and local sales/use taxes. In the event CONTRACTOR fails to pay such California or any other state or local sales/use tax and such taxes have been paid by COUNTY to CONTRACTOR, CONTRACTOR shall reimburse COUNTY for any and all tax amounts paid by COUNTY as a result of such failure and any attorneys' fees, including costs, associated therewith. In addition, CONTRACTOR shall be solely responsible for all taxes based on CONTRACTOR's income or gross revenue, or personal property taxes levied or assessed on CONTRACTOR's personal property to which COUNTY does not hold title.

A.7 FINANCIAL RESOURCES

During the term of this Agreement, CONTRACTOR shall maintain sufficient financial resources necessary to fully perform its obligations. CONTRACTOR confirms there has been no material financial change in CONTRACTOR (including any parent company) since its last financial statement that has resulted in a negative impact to its financial condition.

A.8 DISALLOWANCE

If CONTRACTOR receives payment under this Agreement which is later disallowed by COUNTY for nonconformance with the Agreement, CONTRACTOR shall promptly refund the disallowed amount to COUNTY, or, at its option, COUNTY may offset the amount disallowed from any payment due to CONTRACTOR.

B.1 DPSS RESPONSIBILITIES

DPSS shall:

- a) Submit in writing, through U.S. mail, overnight courier, or email, a scope of work to CONTRACTOR for each project request and/or system enhancement. The scope of work submitted shall include expected deliverables.
- b) Confirm acceptance of each project by returning an executed copy of the Project Estimate to CONTRACTOR. The Project Estimate shall include a statement of work, deliverables, project timeline, and cost.
- c) Request support through the support system (<https://jumpssc.com/>), or by calling 916-357-6779. For support outside normal business hours, or on holidays, COUNTY may contact, Denise Brinkmeyer: 918-625-7335.
- d) Submit Help Desk Tickets (HDTs) to the JUMP Technology Service Support Center (SSC) for system related inquiries. All HDTs submitted to the SSC shall be made in the form of an issue report and shall include the following:
 1. Contact information for the designated COUNTY liaison that reports the problem.
 2. The name and version number of the system being used.
 3. A general description of the operating environment in which the issue was discovered (as applicable).
 4. A description of relevant hardware components in the environment.
 5. A description of relevant software components (O.S., browser) in the environment and versions.
 6. A description of the problem and expected results.
 7. System generated error messages or diagnostics where available.
- e) Maintain an accurate record of all HDT actions, based on feedback from CONTRACTOR.
- f) Monitor the performance of the CONTRACTOR in meeting the terms, conditions and services in this Agreement. DPSS, at its sole discretion, may monitor the performance of the CONTRACTOR through any combination of the following methods: periodic on-site visits, annual inspections, evaluations and CONTRACTOR self-monitoring.

B.2 CONTRACTOR RESPONSIBILITIES

CONTRACTOR shall provide the services as set forth below.

1. Schedule of Maintenance and Support

CONTRACTOR shall provide to the COUNTY Updates (hereinafter "Maintenance") and technical support (hereinafter "Support") in accordance with the terms of this Agreement.

CONTRACTOR shall provide technical support to assist in troubleshooting, defining, and/or executing corrective actions when the COUNTY requires support, as follows:

Deliverables

- a. System Maintenance Efforts
- b. Technical Consulting

- c. Troubleshooting
- d. Interface with COUNTY project designee
- e. System enhancement efforts outside of Standard Maintenance

2. Maintenance and Support Services

a. Definition of Support Services

COUNTY may contact JUMP Technology Services Support Center (SSC) and its Projects Management Office (PMO) or a designated Analyst by telephone, facsimile (fax), and electronic mail (email). The PMO or Analyst shall respond to COUNTY Program inquiries, coordinate resolution of Program problems, including the verification of any reported errors, provide acceptable problem workaround, and communicate with designated COUNTY contacts on status and/or for additional problem information and supply the Error Corrections and/or Update Release, as necessary.

b. Service Parameters

- i. During the Period of Performance, the Software System shall be operational and available to the COUNTY at least 99% of the time in any calendar month. The CONTRACTOR shall provide the COUNTY with reports documenting Uptime and Downtime as requested.
- ii. CONTRACTOR shall notify the COUNTY of periods of Scheduled Downtime at least five days prior to the commencement of such Downtime.

c. Support Plan

CONTRACTOR shall provide support 24 hours a day, 7 days a week, each day of the year. During normal business hours (7:00 a.m. and 7:00 p.m., Central Standard Time (CST), Monday through Friday).

The following holidays will generally be observed:

- New Year's Day
- President's Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving
- Day after Thanksgiving
- Christmas Day
- Day before Christmas

i. Support Services include:

- 1. Access via telephone, website portal, and email
- 2. Three designated COUNTY contacts
- 3. Available Update Releases that ship within the twelve-month period

ii. Web Access includes:

- 1. Submitting program inquiries or reporting program problems
- 2. Access to program technical tips
- 3. Access to program problem and solution list(s)
- 4. Access to available patches

- 5. Review COUNTY call/issue and status
- 6. Review COUNTY maintenance contract status

d. Reporting Cases to the Support Services Center

All Program inquiries or issue reports submitted to JUMP Technology Services via an HDT must be made by a designated COUNTY liaison. HDTs will generally fall into one of four categories:

- i. **Technical Assistance:** Questions about Program usage and installation that do not result in registration of a program defect or enhancement request.
- ii. **Program Defect:** the COUNTY encounters a problem that is determined to be an Error or defect in the Program.
- iii. **Feature Enhancements Requests:** Request for a tool or feature that is not included in the current set of JUMP Technology Services' produced or licensed software or features.
- iv. **Documentation Discrepancies**

e. Definitions of HDT Priorities

- i. Priority Definitions: CONTRACTOR and COUNTY shall work jointly to assign the appropriate priority to all HDT based on the following criteria:

Priority	Conditions
1 – High	Critical business impact. The COUNTY has completed loss of service and work cannot reasonably continue; experiences real or perceived data loss or corruption; or an essential part of the system is unusable for the COUNTY, which results in the inability to use a mission critical application.
2 – Medium	Some business impacts. The problem seriously affects the functionality of the Program but can be circumvented so that the Program can be used; or that the Program as a whole function but that a certain function is somewhat disabled, gives incorrect results or does not conform to the specifications.
3 – Low	Minimal business impact. The COUNTY can circumvent the problem and use the system with only slight inconvenience. The error can be considered insignificant and has no significant effect on the usability of the software, e.g., a small system error or a small error in the documentation. This priority is also used for questions, comments, and requests for enhancements to the software.

- ii. CONTRACTOR shall respond to HDTs within CONTRACTOR's published response time goals as follows for all issue's categories excluding enhancement requests:

Priority	Acknowledgment	Response	Closure of HDT
1 – High	2 business hours	4 business hours	
2 – Medium	1 business day	3 business days	
3 – Low	3 business days	5 business days	

1. **Acknowledgment Time** is the time between the COUNTY reporting the HDT to CONTRACTOR and the time CONTRACTOR gives the COUNTY notice that it acknowledges the situation. These response times apply to HDTs reported via the Web during normal business hours (CST), or via the SCC Support Hot Line. HDTs reported the Web outside of normal business hours (CST) shall adhere to the above times from the start of the next business day.
 2. **Response Time** is the time between the COUNTY reporting the HDT and the time that a PMO or SSC Analyst is assigned and actively working on the HDT.
 3. Requests for enhancements or services beyond the scope of this agreement shall be offered to COUNTY according to the rate set forth in Schedule A, Payment Provisions.
- iii. CONTRACTOR's Undertaking: For each HDT reported by COUNTY, CONTRACTOR undertakes to:
1. Maintain a telephone number for COUNTY to call and report a problem and request assistance.
 2. Confirm receipt of all reports to COUNTY. The confirmation shall be in written form and shall contain an identifying ticket number assigned by the CONTRACTOR, which will be used in all communications and contain a timeframe in which a response from CONTRACTOR can be expected.
 3. Analyze the report and verify the existence of the problem.
 4. Provide COUNTY direction and assistance in resolving technical issues.
- f. **Closure of HDT**
HDT shall be resolved and closed under the following conditions:
- i. COUNTY receives an error correction, a workaround, or information that resolves the issue.
 - ii. Issue is identified as not a problem with the JUMP product.
 - iii. If the HDT results in a defect correction or enhancement request being entered and COUNTY has been notified of the defect/enhancement ID for future reference.
 - iv. COUNTY has not responded after 10 business days to CONTRACTOR after information was provided via a final message left on COUNTY's voice mail or via email. The HDT can be reopened if the issue has not been resolved.
- g. **Software Releases**
The COUNTY's project manager shall publish release information at release planning and implementation. The COUNTY shall also be provided with a link to iteration plans that include requested or planned future enhancements. All updates implemented shall require COUNTY approval.
- h. **Failure Correction Goals**
HDT that result in the identification of a software system defect/failure will cause a Defect to be logged. The COUNTY shall be notified that the defect/failure was received and will be provided with an HDT number. CONTRACTOR shall respond to defect reports as indicated in the table below. The response time goals do not apply in situations where it is verified that the source of the failure is a third-party product.

Defect Correction Goals:

Priority	Interim Solution	Final Solution
1 – High	All commercially reasonable effort until the defect is repaired	Permanent correction within 30 business days of identification of the cause of the defect.
2 – Medium	N/A	Permanent correction within 45 business days of identification of the cause of the defect.
3 – Low	N/A	Permanent correction with next schedule Major Release or Update Release.

3. ENHANCEMENTS/MAINTENANCE & SUPPORT

- a. CONTRACTOR shall provide additional projects as requested by DPSS.
- b. CONTRACTOR shall provide a Project Estimate to COUNTY within ten (10) business days of receipt of the Scope of Work. The Project Estimate shall include a statement of work, deliverables, project timeline, and cost. CONTRACTOR shall provide the Project Estimate to the DPSS Contracts Administration Unit (CAU) in writing, through U.S. mail, overnight courier, or email.
- c. No work shall be completed unless the Project Estimate is formally approved and executed by both parties.

B.3 REPORTING

- a. On a weekly basis and/or as requested, CONTRACTOR shall make available to the COUNTY a complete and secure (i.e. encrypted and appropriated authenticated) download file of COUNTY Data in XML format including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in their native format.
- b. CONTRACTOR shall provide the COUNTY with reports documenting Uptime and Downtime, as requested.
- c. CONTRACTOR shall provide the COUNTY with access to license limit reports each month to assist in monitoring the license level. This report shall be available by the 15th day of each month.

ATTACHMENT I

DPSS 2076A, DPSS 2076B & Instructions

COUNTY OF RIVERSIDE
DEPARTMENT OF PUBLIC SOCIAL SERVICES

CONTRACTOR PAYMENT REQUEST

To: Riverside County
Department of Public Social Services
Attn: Management Reporting
Unit
4060 County Circle Drive
Riverside CA 92503

From: IUMP Technology Services, L.L.C.
Remit to Name
Address
Contractor Name
Contract Number

Total amount requested _____ for the period of _____ 20 _____

Select Payment Type(s) Below:

- Advance Payment \$ _____ (if allowed by Contract/MOU)
- Actual Payment \$ _____ (Same amount as 2076B if needed)
- Unit of Service Payment \$ _____ # of Units) X _____ (\$) _____
- _____ # of Units) X (\$) _____ # of Units) X _____ (\$) _____
- _____ # of Units) X (\$) _____ # of Units) X _____ (\$) _____

Any questions regarding this request should be directed to: _____
Name Phone Number

I hereby certify under penalty of perjury that to the best of my knowledge the above is true and correct

Authorized Signature Title Date

FOR DPSS USE ONLY (DO NOT WRITE BELOW THIS LINE)

Business Unit (5)	Purchase Order # (10)	Invoice #
Account (6)	Amount Authorized	
Fund (5)	If amount authorized is different from amount request, please explain:	
Dept ID (10)	_____	_____
Program (5)	Program (if applicable)	Date
Class (10)	Management Reporting Unit	Date
Project/Grant (15)	Contracts Administration Unit	Date
Vendor Code (10)	General Accounting Section	Date

COUNTY OF RIVERSIDE DEPARTMENT OF PUBLIC SOCIAL SERVICES CONTRACTOR EXPENDITURE REPORT (2076B)				
CONTRACTOR:				
ACTUAL EXPENDITURES FOR (MM/YYYY)				
CONTRACT #:				
EXPENSE CATEGORY	APPROVED BUDGETED AMOUNT	CURRENT EXPENDITURES BILLABLE AMOUNT	CUMULATIVE EXPENDITURES	UNEXPENDED BUDGETED AMOUNT

List each item as outlined in contract budget.

TOTAL BUDGET/EXPENSES				

IN-KIND CASH CONTRIBUTION

List each type of contribution				
TOTAL IN-KIND/CASH MATCH				

CLIENT FEES COLLECTED	CURRENT PERIOD	YEAR TO DATE
-----------------------	----------------	--------------

DEPARTMENT OF PUBLIC SOCIAL SERVICES FORMS

Mailing Instructions: When completed, these forms will summarize all of your claims for payment. Your Claims Packet will include DPSS 2076A, 2076B (if required). invoices, payroll verification, and copies of canceled checks attached, receipts, bank statements, sign-in sheets, daily logs, mileage logs, and other back-up documentation needed to comply with Contract/MOU.

Mail Claims Packet to address shown on upper left corner of DPSS 2076A.
[see method, time, and schedule/condition of payments].
(Please type or print information on all DPSS Forms.)

DPSS 2076A
CONTRACTOR PAYMENT REQUEST

"Remit to Name"
The legal name of your agency.

"Address"
The remit to address used when this contract was established for your agency. All address changes must be submitted for processing prior to use.

"Contractor Name"
Business name, if different than legal name (if not leave blank).

"Contract Number"
Can be found on the first page of your contract.

"Amount Requested"
Fill in the total amount and billing period you are requesting payment for.

"Payment Type"
Check the box and enter the dollar amount for the type(s) of payment(s) you are requesting payment for.

"Any questions regarding..."
Fill in the name and phone number of the person to be contacted should any questions arise regarding your request for payment.

"Authorized Signature, Title, and Date (Contractor's)
Self-explanatory (required). Original Signature needed for payment.
EVERYTHING BELOW THE THICK SOLID LINE IS FOR DPSS USE ONLY AND SHOULD BE LEFT BLANK.

ATTACHMENT II
PII Privacy and Security Standards

I. 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 facilities where 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:
 1. Properly coded key cards
 2. Authorized door keys
 3. 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 systems 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 staff. Visitors to the data center area must be escorted at all times by authorized 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 are multi-use meaning that there are County and non-County 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. Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing PII.

II. 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.
 - 1. All workstations, laptops and other systems, which process and/or store PII, must have critical security patches applied, with system reboot if necessary.
 - 2. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.
 - 3. 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.
 - 4. 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.
 - 1. All users must be issued a unique user name for accessing PII.
 - 2. 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.
 - 3. Passwords are not to be shared.
 - 4. Passwords must be at least eight (8) characters.
 - 5. Passwords must be a non-dictionary word.
 - 6. Passwords must not be stored in readable format on the computer or server.
 - 7. Passwords must be changed every ninety (90) days or less. It is recommended that passwords be required to be changed every sixty (60) days or less.
 - 8. Passwords must be changed if revealed or compromised.
 - 9. 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:
 - 1. Data is confidential;
 - 2. Systems are logged;
 - 3. System use is for business purposes only, by authorized users; and
 - 4. Users shall log off the system immediately if they do not agree with these requirements.
- K. System Logging.
 - 1. 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.
 - 2. 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.
 - 3. If PII is stored in a database, database logging functionality shall be enabled.
 - 4. 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.
 - 1. 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.
 - 2. Encryption can be end to end at the network level, or the data files containing PII can be encrypted.
 - 3. 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.

III. AUDIT CONTROLS

- A. System Security Review.
 - 1. The Contractor must ensure audit control mechanisms are in place.
 - 2. 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.
 - 3. 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.

IV. 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.
 - 1. The Contractor shall have established documented procedures to backup PII to maintain retrievable exact copies of PII.
 - 2. The documented backup procedures shall contain a schedule which includes incremental and full backups.
 - 3. The procedures shall include storing backups offsite.
 - 4. The procedures shall ensure an inventory of backup media.
 - 5. The Contractor shall have established documented procedures to recover PII data.
 - 6. The documented recovery procedures shall include an estimate of the amount of time needed to restore the PII data.

V. 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 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 except for identified routine business purposes or with express written permission of the County.
- G. Faxing.
 - 1. Faxes containing PII shall not be left unattended and fax machines shall be in secure areas.
 - 2. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.
 - 3. Fax numbers shall be verified with the intended recipient before sending the fax.
- H. Mailing.
 - 1. Mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.
 - 2. 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 the County to use another method.

VI. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

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

The Contractor shall immediately notify the County when it discovers that there may have been a breach in security which has or may have resulted in compromise to confidential data. For purposes of this section, immediately is defined as within two hours of discovery. The County contact for such notification is as follows:

Breaches should be referred to:

Civil Rights Coordinator
Riverside County Department of Public Social Services
7894 Mission Grove Parkway, Suite 100
Riverside, CA 92508
(951) 358-6841

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

PREAMBLE

The Department of Health Care Services (DHCS) and the Riverside County of Department of Public Social Services enter into this Medi-Cal Data Privacy and Security Agreement (Agreement) in order to ensure the privacy and security of Medi-Cal Personally Identifiable Information (PII). DHCS receives federal funding to administer California's Medicaid Program (Medi-Cal). County Department assists in the administration of Medi-Cal, in that DHCS and County Department access DHCS eligibility information for the purpose of determining eligibility for Medi-Cal. This Agreement covers the County of Riverside, Department of workers, who assist in the administration of Medi-Cal; and access, use, or disclose Medi-Cal PII.

DEFINITIONS

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

1. "Assist in the Administration of Medi-Cal" is performing an administrative function on behalf of Medi-Cal, and includes, but is not limited to, activities such as establishing eligibility and methods of reimbursement; determining the amount of medical assistance; providing services for recipients; conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of Medi-Cal; and conducting or assisting a legislative investigation or audit related to the administration of Medi-Cal;
2. "Breach" shall have the meaning given to such term under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and its implementing regulations under the Information Practices Act, Civil Code section 1798.29, and under the Agreement between the Social Security Administration (SSA) and DHCS, known as the Information Exchange Agreement (IEA) (Exhibit A); this definition shall include these definitions as set out below and as may be amended in the future:
 - a. "Breach" means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information." (HIPAA Regulation 45.C.F.R. 164.402);
 - b. - Breach of the security of the system' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency." (Civil C. § 1798.23 (d));
 - c. 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 have access or potential access to PII or Covered Information, whether physical, electronic, or in spoken work or recording." (IEA, Attachment 4, Electronic Information Exchange Security Requirements, Guidelines, and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the Social Security Administration, Exhibit. A).

3. "County Worker" means those county employees, contractors, subcontractors, vendors and agents performing job functions for the County that require access to and/or use of Medi-Cal PII and that are authorized by the County to access and use Medi-Cal PII.

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

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

AGREEMENTS

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

I. PRIVACY AND CONFIDENTIALITY

- A. County Department workers covered by this Agreement (County Workers) may use or disclose Medi-Cal PII only as permitted in this Agreement and only to assist in the administration of Medi-Cal in accordance with Welfare and Institutions Code section 14100.2 and 42 Code of Federal Regulations section 431.300 et.seq., or as required by law. Disclosures, which are required by law, such as a court order, or are made with the explicit written authorization of the Medi-Cal client, are allowable. Any other use or disclosure of Medi-Cal PII requires the express approval in writing of DHCS. No County Worker shall duplicate, disseminate or disclose Medi-Cal PII except as allowed in this Agreement.
- B. Pursuant to this Agreement, County Workers may use Medi-Cal PII only to perform administrative functions related to determining eligibility for individuals applying for Medi-Cal.
- C. Access to Medi-Cal PII shall be restricted to only County Workers, who need the Medi-Cal PII to perform their official duties to assist in the administration of Medi-Cal.
- D. County Workers, who access, disclose or use Medi-Cal PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

II. PERSONNEL CONTROLS

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

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

2. Maintain records indicating each County Worker's name and the date on which the privacy and security awareness training was completed;
3. Retain the most recent training records for a period of three years after completion of the training.

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

C. **Confidentiality Statement.** Ensure that all County Workers, who assist in the administration of Medi-Cal, and use or disclose Medi-Cal PII, sign a confidentiality statement. The statement shall include at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement shall be signed by County Workers prior to accessing Medi-Cal PII and the most recent version shall be retained for a period of three years.

D. **Background Check.** Conduct a background screening of a County Worker before a County Worker may access DHCS PII. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees, who are authorized to bypass significant technical and operational security controls. County Department shall retain each County Worker's most recent background check documentation for a period of three years.

III. MANAGEMENT OVERSIGHT AND MONITORING

County Department agrees to:

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

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

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

IV. INFORMATION SECURITY AND PRIVACY STAFFING

The County agrees to:

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

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

V. PHYSICAL SECURITY

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

A. Secure all areas of County Department facilities where County Workers assist in the administration of Medi-Cal and use or disclose Medi-Cal PII. The County Department shall ensure these secured areas

are only accessed by authorized individuals with properly coded key cards, authorized door keys or access authorization; and access to premises is by official identification.

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

C. Ensure each physical location, where Medi-Cal PII is used or stored, has procedures and controls that ensure an individual, who is terminated from access to the facility is promptly escorted from the facility by an authorized employee and access is revoked.

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

E. Ensure data centers with servers, data storage devices, and critical network infrastructure involved in the use or storage of Medi-Cal PII have perimeter security and access controls that limit access to only authorized Information Technology (IT) staff. Visitors to the data center area must be escorted by authorized IT staff at all times.

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

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

VI. TECHNICAL SECURITY CONTROLS

A. Workstation/Laptop encryption. All workstations and laptops, which store Medi-Cal PII either directly or temporarily, must be encrypted using a FIPS 140-2 certified algorithm 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk.

B. Server Security. Servers containing unencrypted Medi-Cal PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

C. Minimum Necessary. Only the minimum necessary amount of Medi-Cal PII required to perform necessary business functions may be copied, downloaded, or exported.

D. Removable media devices. All electronic files, which contain Medi-Cal PII data, must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128bit or higher, such as AES.

E. Antivirus software. All workstations, laptops and other systems, which process and/or store Medi-Cal PII, must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

F. Patch Management. All workstations, laptops and other systems, which process and/or store Medi-Cal PII, must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches deemed as high risk must be installed within 30 days of vendor release. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.

G. User IDs and Password Controls. All users must be issued a unique user name for accessing Medi-Cal PII. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

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

H. User Access. Exercise management control and oversight, in conjunction with DHCS, of the function of authorizing individual user access to Social Security Administration (SSA) data, MEDS, and over the process of issuing and maintaining access control numbers and passwords.

I. Data Destruction. When no longer needed, all Medi-Cal PII must be wiped using the Gutmann or U.S. Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88.

J. System Timeout. The system providing access to Medi-Cal PII must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

K. Warning Banners. All systems providing access to Medi-Cal PII must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

L. System Logging. The system must maintain an automated audit trail that can identify the user or system process, initiates a request for Medi-Cal PII, or alters Medi-Cal PII. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If Medi-Cal PII is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three years after occurrence.

M. Access Controls. The system providing access to Medi-Cal PII must use role based access controls for all user authentications, enforcing the principle of least privilege.

N. Transmission encryption. All data transmissions of Medi-Cal PII outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm that is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing Medi-Cal PII can be encrypted. This requirement pertains to any type of Medi-Cal PII in motion such as website access, file transfer, and E-Mail.

O. Intrusion Detection. All systems involved in accessing, holding, transporting, and protecting Medi-Cal PII, which are accessible through the Internet, must be protected by a comprehensive intrusion detection and prevention solution.

VII. AUDIT CONTROLS

A. System Security Review. County Department must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing Medi-Cal PII must have at least an annual system risk assessment/security review that ensures administrative, physical, and technical controls are functioning effectively and provide an adequate levels of protection. Reviews should include vulnerability scanning tools.

B. Log Reviews. All systems processing and/or storing Medi-Cal PII must have a routine procedure in place to review system logs for unauthorized access.

C. Change Control. All systems processing and/or storing Medi-Cal PII must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

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

VIII. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

A. Emergency Mode Operation Plan. County Department must establish a documented plan to enable continuation of critical business processes and protection of the security of Medi-Cal PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

B. Data Centers. Data centers with servers, data storage devices, and critical network infrastructure involved in the use or storage of Medi-Cal PII, must include sufficient environmental protection such as cooling, power, and fire prevention, detection, and suppression.

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

IX. PAPER DOCUMENT CONTROLS

A. Supervision of Data. Medi-Cal PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. Medi-Cal PII in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

B. Escorting Visitors. Visitors to areas where Medi-Cal PII is contained shall be escorted and Medi-Cal PII shall be kept out of sight while visitors are in the area.

C. Confidential Destruction. Medi-Cal PII must be disposed of through confidential means, such as cross cut shredding and pulverizing.

D. Removal of Data. Medi-Cal P11 must not be removed from the premises of County Department except for identified routine business purposes or with express written permission of DHCS.

E. Faxing. Faxes containing Medi-Cal PII shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

F. Mailing. Mailings containing Medi-Cal PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible. Mailings that include 500 or more individually identifiable records containing Medi-Cal PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt, unless the prior written permission of DHCS to use another method is obtained.

X. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

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

A. Initial Notice to DHCS. (1) To notify DHCS **immediately by telephone call plus email or fax** upon the discovery of a breach of unsecured Medi-Cal PII in electronic media or in any other media if the PII was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to DHCS by the SSA. (2) To notify DHCS **within 24 hours by email or fax** of the discovery of any breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by County Department as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach), who is an employee, officer or other agent of County Department. Notice shall be provided to the DHCS Program Contract Manager, the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PII, notice shall be provided by calling the DHCS ITSD Service Desk. Notice shall be made using the "DHCS Privacy Incident Report" form, including all information known at the time. County Department shall use the most current version of this form, which is posted on the DHCS Privacy Office website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "County Use" near the middle of the page) or use this link:

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

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

1. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
2. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

B. Investigation and Investigative Report. To immediately investigate a breach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PII, within 72 hours of the discovery, County Department shall submit an updated "DHCS Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the DHCS

Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer.

C. Complete Report. To provide a complete report of the investigation to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer within ten working days of the discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure. The report shall be submitted on the "DHCS Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If DHCS requests information in addition to that listed on the "DHCS Privacy Incident Report" form, County Department shall make reasonable efforts to provide DHCS with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "DHCS Privacy Incident Report" form. DHCS will review and approve the determination of whether a breach occurred, and individual notifications are required, and the corrective action plan.

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

E. Responsibility for Reporting of Breaches. If the cause of a breach of Medi-Cal PII is attributable to County Department or its agents, subcontractors or vendors, County Department is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary, U.S. Department of Health and Human Services. If a breach of unsecured PII involves more than 500 residents of the State of California or its jurisdiction, County Department shall notify the federal Secretary, Department of Health and Human Services, of the breach immediately upon discovery of the breach. If County Department has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to DHCS in addition to County Department, County Department shall notify DHCS, and DHCS and County Department may take appropriate action to prevent duplicate reporting.

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

**DHCS Program Contract
Manager
DHCS Privacy Officer
DHCS Information
Security Officer**

Program Integrity and Security Unit Privacy Officer Information Security Officer
Policy Operations Branch do: Office of HIPAA Compliance DHCS Information Security
Medi-Cal Eligibility Division DHCS Privacy Office, MS 4722 Office, MS 6400
1501 Capitol Avenue, MS 4607 P.O. Box 997413 P.O. Box 997413

P.O. Box 997417 Sacramento, CA 95899-7413 Sacramento, CA 95899-7413
Sacramento, CA 95899-7417

Email: Email: iso@dhcs.ca.gov
Telephone: (916) 552-9200 privacyofficerdhcs.ca.cov Fax: (916) 440-5537
Telephone: (916) 445-4646 Telephone:
Fax: (916) 440-7680 ITSD Service Desk
(916) 440-7000 or (800) 579-0874

XI. COMPLIANCE WITH SSA AGREEMENT

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

XII. COUNTY DEPARTMENT'S AGENTS AND SUBCONTRACTORS

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

XIII. ASSESSMENTS AND REVIEWS

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

XIV. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

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

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

XV. AMENDMENT OF AGREEMENT

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

XVI. TERMINATION

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

XVII. TERMINATION FOR CAUSE

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

XVIII. SIGNATORIES

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this Agreement. The authorized officials whose signatures appear below have committed their respective agencies to the terms of this Agreement. The contract is effective on the day the final signature is obtained.

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

ATTACHMENT IV
HIPAA Business Associate AgreementHIPAA Business Associate Agreement
Addendum to Contract
Between the County of Riverside and Unassigned

This HIPAA Business Associate Agreement (the "Addendum") supplements, and is made part of (the DPSS-0002444 "Underlying Agreement") between the County of Riverside ("County") and JUMP Technology Services, L.L.C. ("Contractor") and shall be effective as of the date the Underlying Agreement is approved by both Parties (the "Effective Date").

RECITALS

WHEREAS, County and Contractor entered into the Underlying Agreement pursuant to which the Contractor provides services to County, and in conjunction with the provision of such services certain protected health information ("PHI") and/or certain electronic protected health information ("ePHI") may be created by or made available to Contractor for the purposes of carrying out its obligations under the Underlying Agreement; and,

WHEREAS, the provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191 enacted August 21, 1996, and the Health Information Technology for Economic and Clinical Health Act ("HITECH") of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 enacted February 17, 2009, and the laws and regulations promulgated subsequent thereto, as may be amended from time to time, are applicable to the protection of any use or disclosure of PHI and/or ePHI pursuant to the Underlying Agreement; and,

WHEREAS, County is a covered entity, as defined in the Privacy Rule; and,

WHEREAS, to the extent County discloses PHI and/or ePHI to Contractor or Contractor creates, receives, maintains, transmits, or has access to PHI and/or ePHI of County, Contractor is a business associate, as defined in the Privacy Rule; and,

WHEREAS, pursuant to 42 USC §17931 and §17934, certain provisions of the Security Rule and Privacy Rule apply to a business associate of a covered entity in the same manner that they apply to the covered entity, the additional security and privacy requirements of HITECH are applicable to business associates and must be incorporated into the business associate agreement, and a business associate is liable for civil and criminal penalties for failure to comply with these security and/or privacy provisions; and,

WHEREAS, the parties mutually agree that any use or disclosure of PHI and/or ePHI must be in compliance with the Privacy Rule, Security Rule, HIPAA, HITECH and any other applicable law; and,

WHEREAS, the parties intend to enter into this Addendum to address the requirements and obligations set forth in the Privacy Rule, Security Rule, HITECH and HIPAA as they apply to Contractor as a business associate of County, including the establishment of permitted and required uses and disclosures of PHI and/or ePHI created or received by Contractor during the course of performing functions, services and activities on behalf of County, and appropriate limitations and conditions on such uses and disclosures;

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the parties agree as follows:

1. **Definitions.** Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in HITECH, HIPAA, Security Rule and/or Privacy Rule, as may be amended from time to time.
- A. "Breach" when used in connection with PHI means the acquisition, access, use or disclosure of PHI in a manner not permitted under subpart E of the Privacy Rule which compromises the security or privacy of the PHI, and shall have the meaning given such term in 45 CFR §164.402.
 - (1) Except as provided below in Paragraph (2) of this definition, acquisition, access, use, or disclosure of PHI in a manner not permitted by subpart E of the Privacy Rule is presumed to be a breach unless Contractor demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following four factors:
 - (a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
 - (b) The unauthorized person who used the PHI or to whom the disclosure was made;
 - (c) Whether the PHI was actually acquired or viewed; and
 - (d) The extent to which the risk to the PHI has been mitigated.
 - (2) Breach excludes:
 - (a) Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of the Privacy Rule.
 - (b) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate, or organized health care arrangement in which County participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by subpart E of the Privacy Rule.
 - (c) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- B. "Business associate" has the meaning given such term in 45 CFR §164.501, including but not limited to a subcontractor that creates, receives, maintains, transmits or accesses PHI on behalf of the business associate.
- C. "Data aggregation" has the meaning given such term in 45 CFR §164.501.

- D. "Designated record set" as defined in 45 CFR §164.501 means a group of records maintained by or for a covered entity that may include: the medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or, used, in whole or in part, by or for the covered entity to make decisions about individuals.
- E. "Electronic protected health information" ("ePHI") as defined in 45 CFR §160.103 means protected health information transmitted by or maintained in electronic media.
- F. "Electronic health record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff, and shall have the meaning given such term in 42 USC §17921(5).
- G. "Health care operations" has the meaning given such term in 45 CFR §164.501.
- H. "Individual" as defined in 45 CFR §160.103 means the person who is the subject of protected health information.
- I. "Person" as defined in 45 CFR §160.103 means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.
- J. "Privacy Rule" means the HIPAA regulations codified at 45 CFR Parts 160 and 164, Subparts A 17 and E.
- K. "Protected health information" ("PHI") has the meaning given such term in 45 CFR §160.103, which includes ePHI.
- L. "Required by law" has the meaning given such term in 45 CFR §164.103.
- M. "Secretary" means the Secretary of the U.S. Department of Health and Human Services 22 ("HHS").
- N. "Security incident" as defined in 45 CFR §164.304 means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- O. "Security Rule" means the HIPAA Regulations codified at 45 CFR Parts 160 and 164, Subparts 27 A and C.
- P. "Subcontractor" as defined in 45 CFR §160.103 means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
- Q. "Unsecured protected health information" and "unsecured PHI" as defined in 45 CFR §164.402 means PHI not rendered unusable, unreadable, or indecipherable to unauthorized persons through use of a technology or methodology specified by the Secretary in the guidance issued 34 under 42 USC §17932(h)(2).

2. Scope of Use and Disclosure by Contractor of County's PHI and/or ePHI.

- A. Except as otherwise provided in this Addendum, Contractor may use, disclose, or access PHI and/or ePHI as necessary to perform any and all obligations of Contractor under the Underlying Agreement or to perform functions, activities or services for, or on behalf of, County as specified in this Addendum, if such use or disclosure does not violate HIPAA, HITECH, the Privacy Rule and/or Security Rule.
- B. Unless otherwise limited herein, in addition to any other uses and/or disclosures permitted or authorized by this Addendum or required by law, in accordance with 45 CFR §164.504(e)(2), Contractor may:
 - (1) Use PHI and/or ePHI if necessary, for Contractor's proper management and administration and to carry out its legal responsibilities; and,
 - (2) Disclose PHI and/or ePHI for the purpose of Contractor's proper management and administration or to carry out its legal responsibilities, only if:
 - (a) The disclosure is required by law; or,
 - (b) Contractor obtains reasonable assurances, in writing, from the person to whom Contractor will Hold such PHI disclose such PHI and/or ePHI that the person will:
 - (i) and/or ePHI in confidence and use or further disclose it only for the purpose for which Contractor disclosed it to the person, or as required by law; and,
 - (ii) Notify Contractor of any instances of which it becomes aware in which the confidentiality of the information has been breached; and,
 - (3) Use PHI to provide data aggregation services relating to the health care operations of County pursuant to the Underlying Agreement or as requested by County; and,
 - (4) De-identify all PHI and/or ePHI of County received by Contractor under this Addendum provided that the de-identification conforms to the requirements of the Privacy Rule and/or 24 Security Rule and does not preclude timely payment and/or claims processing and receipt.
- C. Notwithstanding the foregoing, in any instance where applicable state and/or federal laws and/or regulations are more stringent in their requirements than the provisions of HIPAA, including, but not limited to, prohibiting disclosure of mental health and/or substance abuse records, the applicable state and/or federal laws and/or regulations shall control the disclosure of records.

3. Prohibited Uses and Disclosures.

- A. Contractor may neither use, disclose, nor access PHI and/or ePHI in a manner not authorized by the Underlying Agreement or this Addendum without patient authorization or de-identification of the PHI and/or ePHI and as authorized in writing from County.
- B. Contractor may neither use, disclose, nor access PHI and/or ePHI it receives from County or from another business associate of County, except as permitted or required by this Addendum, or as required by law.

- C. Contractor agrees not to make any disclosure of PHI and/or ePHI that County would be prohibited from making.
- D. Contractor shall not use or disclose PHI for any purpose prohibited by the Privacy Rule, Security Rule, HIPAA and/or HITECH, including, but not limited to 42 USC §17935 and §17936. Contractor agrees:
 - (1) Not to use or disclose PHI for fundraising, unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.514(f) or 45 CFR §164.508;
 - (2) Not to use or disclose PHI for marketing, as defined in 45 CFR §164.501, unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.508(a)(3);
 - (3) Not to disclose PHI, except as otherwise required by law, to a health plan for purposes of carrying out payment or health care operations, if the individual has requested this restriction pursuant to 42 USC §17935(a) and 45 CFR §164.522, and has paid out of pocket in full for the health care item or service to which the PHI solely relates; and,
 - (4) Not to receive, directly or indirectly, remuneration in exchange for PHI, or engage in any act that would constitute a sale of PHI, as defined in 45 CFR §164.502(a)(5)(ii), unless permitted by the Underlying Agreement and in compliance with the requirements of a valid authorization under 45 CFR §164.508(a)(4). This prohibition shall not apply to payment by County to Contractor for services provided pursuant to the Underlying Agreement.

4. **Obligations of County.**

- A. County agrees to make its best efforts to notify Contractor promptly in writing of any restrictions on the use or disclosure of PHI and/or ePHI agreed to by County that may affect Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.
- B. County agrees to make its best efforts to promptly notify Contractor in writing of any changes in, or revocation of, permission by any individual to use or disclose PHI and/or ePHI, if such changes or revocation may affect Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.
- C. County agrees to make its best efforts to promptly notify Contractor in writing of any known limitation(s) in its notice of privacy practices to the extent that such limitation may affect Contractor's use or disclosure of PHI and/or ePHI.
- D. County agrees not to request Contractor to use or disclose PHI and/or ePHI in any manner that would not be permissible under HITECH, HIPAA, the Privacy Rule, and/or Security Rule.
- E. County agrees to obtain any authorizations necessary for the use or disclosure of PHI and/or ePHI, so that Contractor can perform its obligations under this Addendum and/or Underlying Agreement.

5. **Obligations of Contractor.** In connection with the use or disclosure of PHI and/or ePHI, Contractor agrees to:
- A. Use or disclose PHI only if such use or disclosure complies with each applicable requirement of 45 CFR §164.504(e). Contractor shall also comply with the additional privacy requirements that are applicable to covered entities in HITECH, as may be amended from time to time.
 - B. Not use or further disclose PHI and/or ePHI other than as permitted or required by this Addendum or as required by law. Contractor shall promptly notify County if Contractor is required by law to disclose PHI and/or ePHI.
 - C. Use appropriate safeguards and comply, where applicable, with the Security Rule with respect to ePHI, to prevent use or disclosure of PHI and/or ePHI other than as provided for by this Addendum.
 - D. Mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of PHI and/or ePHI by Contractor in violation of this Addendum.
 - E. Report to County any use or disclosure of PHI and/or ePHI not provided for by this Addendum or otherwise in violation of HITECH, HIPAA, the Privacy Rule, and/or Security Rule of which Contractor becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410.
 - F. In accordance with 45 CFR §164.502(e)(1)(ii), require that any subcontractors that create, receive, maintain, transmit or access PHI on behalf of the Contractor agree through contract to the same restrictions and conditions that apply to Contractor with respect to such PHI and/or ePHI, including the restrictions and conditions pursuant to this Addendum.
 - G. Make available to County or the Secretary, in the time and manner designated by County or Secretary, Contractor's internal practices, books and records relating to the use, disclosure and privacy protection of PHI received from County, or created or received by Contractor on behalf of County, for purposes of determining, investigating or auditing Contractor's and/or County's compliance with the Privacy Rule.
 - H. Request, use or disclose only the minimum amount of PHI necessary to accomplish the intended purpose of the request, use or disclosure in accordance with 42 USC §17935(b) and 45 CFR §164.502(b)(1).
 - I. Comply with requirements of satisfactory assurances under 45 CFR §164.512 relating to notice or qualified protective order in response to a third party's subpoena, discovery request, or other lawful process for the disclosure of PHI, which Contractor shall promptly notify County upon Contractor's receipt of such request from a third party.
 - J. Not require an individual to provide patient authorization for use or disclosure of PHI as a condition for treatment, payment, enrollment in any health plan (including the health plan administered by County), or eligibility of benefits, unless otherwise excepted under 45 CFR §164.508(b)(4) and authorized in writing by County.
 - K. Use appropriate administrative, technical and physical safeguards to prevent inappropriate use, disclosure, or access of PHI and/or ePHI.

- L. Obtain and maintain knowledge of applicable laws and regulations related to HIPAA and HITECH, as may be amended from time to time.
 - M. Comply with the requirements of the Privacy Rule that apply to the County to the extent Contractor is to carry out County's obligations under the Privacy Rule.
 - N. Take reasonable steps to cure or end any pattern of activity or practice of its subcontractor of which Contractor becomes aware that constitute a material breach or violation of the subcontractor's obligations under the business associate contract with Contractor, and if such steps are unsuccessful, Contractor agrees to terminate its contract with the subcontractor if feasible.
6. **Access to PHI, Amendment and Disclosure Accounting.** Contractor agrees to:
- A. **Access to PHI, including ePHI.** Provide access to PHI, including ePHI if maintained electronically, in a designated record set to County or an individual as directed by County, within five (5) days of request from County, to satisfy the requirements of 45 CFR §164.524.
 - B. **Amendment of PHI.** Make PHI available for amendment and incorporate amendments to PHI in a designated record set County directs or agrees to at the request of an individual, within fifteen (15) days of receiving a written request from County, in accordance with 45 CFR §164.526.
 - C. **Accounting of disclosures of PHI and electronic health record.** Assist County to fulfill its obligations to provide accounting of disclosures of PHI under 45 CFR §164.528 and, where applicable, electronic health records under 42 USC §17935(c) if Contractor uses or maintains electronic health records. Contractor shall:
 - (1) Document such disclosures of PHI and/or electronic health records, and information related to such disclosures, as would be required for County to respond to a request by an individual for an accounting of disclosures of PHI and/or electronic health record in accordance with 45 CFR §164.528.
 - (2) Within fifteen (15) days of receiving a written request from County, provide to County or any individual as directed by County information collected in accordance with this section to permit County to respond to a request by an individual for an accounting of disclosures of PHI and/or electronic health record.
 - (3) Make available for County information required by this Section 6.C for six (6) years preceding the individual's request for accounting of disclosures of PHI, and for three (3) years preceding the individual's request for accounting of disclosures of electronic health record.
7. **Security of ePHI.** In the event County discloses ePHI to Contractor or Contractor needs to create, receive, maintain, transmit or have access to County ePHI, in accordance with 42 USC §17931 and 45 CFR §164.314(a)(2)(i), and §164.306, Contractor shall:
- A. Comply with the applicable requirements of the Security Rule, and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that Contractor creates, receives, maintains, or transmits on behalf of County in accordance with 45 CFR §164.308, §164.310, and §164.312;

- B. Comply with each of the requirements of 45 CFR §164.316 relating to the implementation of policies, procedures and documentation requirements with respect to ePHI;
 - C. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
 - D. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the Privacy Rule;
 - E. Ensure compliance with the Security Rule by Contractor's workforce;
 - F. In accordance with 45 CFR §164.308(b)(2), require that any subcontractors that create, receive, maintain, transmit, or access ePHI on behalf of Contractor agree through contract to the same restrictions and requirements contained in this Addendum and comply with the applicable requirements of the Security Rule;
 - G. Report to County any security incident of which Contractor becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410; and,
 - H. Comply with any additional security requirements that are applicable to covered entities in Title 42 (Public Health and Welfare) of the United States Code, as may be amended from time to time, including but not limited to HITECH.
8. **Breach of Unsecured PHI.** In the case of breach of unsecured PHI, Contractor shall comply with the applicable provisions of 42 USC §17932 and 45 CFR Part 164, Subpart D, including but not limited to 45 CFR §164.410.
- A. **Discovery and notification.** Following the discovery of a breach of unsecured PHI, Contractor shall notify County in writing of such breach without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, except as provided in 45 CFR §164.412.
- (1) **Breaches treated as discovered.** A breach is treated as discovered by Contractor as of the first day on which such breach is known to Contractor or, by exercising reasonable diligence, would have been known to Contractor, which includes any person, other than the person committing the breach, who is an employee, officer, or other agent of Contractor (determined in accordance with the federal common law of agency).
 - (2) **Content of notification.** The written notification to County relating to breach of unsecured PHI shall include, to the extent possible, the following information if known (or can be reasonably obtained) by Contractor:
 - (a) The identification of each individual whose unsecured PHI has been, or is reasonably believed by Contractor to have been accessed, acquired, used or disclosed during the breach;
 - (b) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
 - (c) A description of the types of unsecured PHI involved in the breach, such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved;

- (d) Any steps individuals should take to protect themselves from potential harm resulting from the breach;
 - (e) A brief description of what Contractor is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,
 - (f) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.
- B. **Cooperation.** With respect to any breach of unsecured PHI reported by Contractor, Contractor shall cooperate with County and shall provide County with any information requested by County to enable County to fulfill in a timely manner its own reporting and notification obligations, including but not limited to providing notice to individuals, prominent media outlets and the Secretary in accordance with 42 USC §17932 and 45 CFR §164.404, §164.406 and §164.408.
- C. **Breach log.** To the extent breach of unsecured PHI involves less than 500 individuals, Contractor shall maintain a log or other documentation of such breaches and provide such log or other documentation on an annual basis to County not later than fifteen (15) days after the end of each calendar year for submission to the Secretary.
- D. **Delay of notification authorized by law enforcement.** If Contractor delays notification of breach of unsecured PHI pursuant to a law enforcement official's statement that required notification, notice or posting would impede a criminal investigation or cause damage to national security, Contractor shall maintain documentation sufficient to demonstrate its compliance with the requirements of 45 CFR §164.412.
- E. **Payment of costs.** With respect to any breach of unsecured PHI caused solely by the Contractor's failure to comply with one or more of its obligations under this Addendum and/or the provisions of HITECH, HIPAA, the Privacy Rule or the Security Rule, Contractor agrees to pay any and all costs associated with providing all legally required notifications to individuals, media outlets, and the Secretary. This provision shall not be construed to limit or diminish Contractor's obligations to indemnify, defend and hold harmless County under Section 9 of this Addendum.
- F. **Documentation.** Pursuant to 45 CFR §164.414(b), in the event Contractor's use or disclosure of PHI and/or ePHI violates the Privacy Rule, Contractor shall maintain documentation sufficient to demonstrate that all notifications were made by Contractor as required by 45 CFR Part 164, Subpart D, or that such use or disclosure did not constitute a breach, including Contractor's completed risk assessment and investigation documentation.
- G. **Additional State Reporting Requirements.** The parties agree that this Section 8.G applies only if and/or when County, in its capacity as a licensed clinic, health facility, home health agency, or hospice, is required to report unlawful or unauthorized access, use, or disclosure of medical information under the more stringent requirements of California Health & Safety Code §1280.15. For purposes of this Section 8.G, "unauthorized" has the meaning given such term in California Health & Safety Code §1280.15(j)(2).
- (1) Contractor agrees to assist County to fulfill its reporting obligations to affected patients and to the California Department of Public Health ("CDPH") in a timely manner under the California Health & Safety Code §1280.15.

- (2) Contractor agrees to report to County any unlawful or unauthorized access, use, or disclosure of patient's medical information without unreasonable delay and no later than two (2) business days after Contractor detects such incident. Contractor further agrees such report shall be made in writing, and shall include substantially the same types of information listed above in Section 8.A.2 (Content of Notification) as applicable to the unlawful or unauthorized access, use, or disclosure as defined above in this section, understanding and acknowledging that the term "breach" as used in Section 8.A.2 does not apply to California Health & Safety Code §1280.15.

9. **Hold Harmless/Indemnification.**

- A. Contractor agrees to indemnify and hold harmless County, all Agencies, Districts, Special Districts and Departments of County, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents and representatives from any liability whatsoever, based or asserted upon any services of Contractor, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this Addendum, including but not limited to property damage, bodily injury, death, or any other element of any kind or nature whatsoever arising from the performance of Contractor, its officers, agents, employees, subcontractors, agents or representatives from this Addendum. Contractor shall defend, at its sole expense, all costs and fees, including but not limited to attorney fees, cost of investigation, defense and settlements or awards, of County, all Agencies, Districts, Special Districts and Departments of County, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents or representatives in any claim or action based upon such alleged acts or omissions.
- B. With respect to any action or claim subject to indemnification herein by Contractor, Contractor shall, at their sole cost, have the right to use counsel of their choice, subject to the approval of County, which shall not be unreasonably withheld, and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of County; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes Contractor's indemnification to County as set forth herein. Contractor's obligation to defend, indemnify and hold harmless County shall be subject to County having given Contractor written notice within a reasonable period of time of the claim or of the commencement of the related action, as the case may be, and information and reasonable assistance, at Contractor's expense, for the defense or settlement thereof. Contractor's obligation hereunder shall be satisfied when Contractor has provided to County the appropriate form of dismissal relieving County from any liability for the action or claim involved.
- C. The specified insurance limits required in the Underlying Agreement of this Addendum shall in no way limit or circumscribe Contractor's obligations to indemnify and hold harmless County herein from third party claims arising from issues of this Addendum.
- D. In the event there is conflict between this clause and California Civil Code §2782, this clause shall be interpreted to comply with Civil Code §2782. Such interpretation shall not relieve the Contractor from indemnifying County to the fullest extent allowed by law.
- E. In the event there is a conflict between this indemnification clause and an indemnification clause contained in the Underlying Agreement of this Addendum, this indemnification shall only apply to the subject issues included within this Addendum.

10. **Term.** This Addendum shall commence upon the Effective Date and shall terminate when all PHI and/or ePHI provided by County to Contractor, or created or received by Contractor on behalf of County, is destroyed or returned to County, or, if it is infeasible to return or destroy PHI and/ePHI, protections are extended to such information, in accordance with section 11.B of this Addendum.
11. **Termination.**
 - A. **Termination for Breach of Contract.** A breach of any provision of this Addendum by either party shall constitute a material breach of the Underlying Agreement and will provide grounds for terminating this Addendum and the Underlying Agreement with or without an opportunity to cure the breach, notwithstanding any provision in the Underlying Agreement to the contrary. Either party, upon written notice to the other party describing the breach, may take any of the following actions:
 - (1) Terminate the Underlying Agreement and this Addendum, effective immediately, if the other party breaches a material provision of this Addendum.
 - (2) Provide the other party with an opportunity to cure the alleged material breach and in the event the other party fails to cure the breach to the satisfaction of the non-breaching party in a timely manner, the non-breaching party has the right to immediately terminate the Underlying Agreement and this Addendum.
 - (3) If termination of the Underlying Agreement is not feasible, the breaching party, upon the request of the non-breaching party, shall implement, at its own expense, a plan to cure the breach and report regularly on its compliance with such plan to the non-breaching party.
 - B. **Effect of Termination.**
 - (1) Upon termination of this Addendum, for any reason, Contractor shall return or, if agreed to in writing by County, destroy all PHI and/or ePHI received from County, or created or received by the Contractor on behalf of County, and, in the event of destruction, Contractor shall certify such destruction, in writing, to County. This provision shall apply to all PHI and/or ePHI which are in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of PHI and/or ePHI, except as provided below in paragraph (2) of this section.
 - (2) In the event that Contractor determines that returning or destroying the PHI and/or ePHI is not feasible, Contractor shall provide written notification to County of the conditions that make such return or destruction not feasible. Upon determination by Contractor that return or destruction of PHI and/or ePHI is not feasible, Contractor shall extend the protections of this Addendum to such PHI and/or ePHI and limit further uses and disclosures of such PHI and/or ePHI to those purposes which make the return or destruction not feasible, for so long as Contractor maintains such PHI and/or ePHI.
12. **General Provisions.**
 - A. **Retention Period.** Whenever Contractor is required to document or maintain documentation pursuant to the terms of this Addendum, Contractor shall retain such documentation for 6 years from the date of its creation or as otherwise prescribed by law, whichever is later.

- B. **Amendment.** The parties agree to take such action as is necessary to amend this Addendum from time to time as is necessary for County to comply with HITECH, the Privacy Rule, Security Rule, and HIPAA generally.
- C. **Survival.** The obligations of Contractor under Sections 3, 5, 6, 7, 8, 9, 11.B and 12.A of this Addendum shall survive the termination or expiration of this Addendum.
- D. **Regulatory and Statutory References.** A reference in this Addendum to a section in HITECH, HIPAA, the Privacy Rule and/or Security Rule means the section(s) as in effect or as amended.
- E. **Conflicts.** The provisions of this Addendum shall prevail over any provisions in the Underlying Agreement that conflict or appear inconsistent with any provision in this Addendum.
- F. **Interpretation of Addendum.**
 - (1) This Addendum shall be construed to be part of the Underlying Agreement as one document. The purpose is to supplement the Underlying Agreement to include the requirements of the Privacy Rule, Security Rule, HIPAA and HITECH.
 - (2) Any ambiguity between this Addendum and the Underlying Agreement shall be resolved to permit County to comply with the Privacy Rule, Security Rule, HIPAA and HITECH generally.
- G. **Notices to County.** All notifications required to be given by Contractor to County pursuant to the terms of this Addendum shall be made in writing and delivered to the County both by fax and to both of the addresses listed below by either registered or certified mail return receipt requested or guaranteed overnight mail with tracing capability, or at such other address as County may hereafter designate. All notices to County provided by Contractor pursuant to this Section shall be deemed given or made when received by County.

County HIPAA Privacy Officer: HIPAA Privacy Manager

County HIPAA Privacy Officer Address: P.O. Box 1569
Riverside, CA 92502

County HIPAA Privacy Officer Fax Number: (951) 955-HIPAA or (951) 955-4472

----- **TO BE COMPLETED BY COUNTY PERSONNEL ONLY** -----

County Departmental Officer: _____

County Departmental Officer Title: _____

County Department Address: _____

County Department Fax Number: _____