SUBMITTAL TO THE RIVERSIDE COUNTY
IN-HOME SUPPORTIVE SERVICES PUBLIC AUTHORITY
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

ITEM
7.2
(ID # 5731)

MEETING DATE:
Tuesday, December 12, 2017

FROM : DPSS In-Home Supportive Services:

SUBJECT: DEPARTMENT OF PUBLIC SOCIAL SERVICES / IN-HOME SUPPORTIVE SERVICES - PUBLIC AUTHORITY: Approve and execute Memorandums of Understanding (MOUs) with IEHP and Molina Healthcare for coordination of services with managed care systems, for five (5) years. [Districts: All]; [Total cost $0]

RECOMMENDED MOTION: That the IHSS-Public Authority Board of Directors:

1. Approve and authorize the Chairman to execute the attached Riverside County In-Home Supportive Services - Public Authority MOUs #PA-03810 with Inland Empire Health Plan (IEHP) and #PA-03811 with Molina Healthcare of California, Partner Plan, Inc., for coordination of services with managed care systems, for five years, effective January 1, 2018;
2. Authorize the Director of the Department of Public Social Services (DPSS) to administer the agreements;
3. Authorize the Purchasing Agent, in accordance with Ordinance NO. 459 and as approved by County Counsel, to: sign amendments that do not change the substantive terms of the agreement.

ACTION: Policy

Susan Von Zabern, Director of Public Social Services 11/22/2017

MINUTES OF THE BOARD OF DIRECTORS

On motion of Director Tavaglione, seconded by Director Jeffries and duly carried, IT WAS ORDERED that the above matter is approved as recommended.

Ayes:	Jeffries, Tavaglione, Perez and Ashley
Nays:	None
Absent:	Washington
Date:	December 12, 2017
xc:	DPSS/IHSS, Purchasing

Kecia Harper-Ihem
Clerk of the Board
By: _____
Deputy

SUBMITTAL TO THE RIVERSIDE COUNTY IN-HOME SUPPORTIVE SERVICES PUBLIC AUTHORITY
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost
COST	$ 0	$ 0	$ 0	$ 0
NET COUNTY COST	$ 0	$ 0	$ 0	$ 0

SOURCE OF FUNDS: Federal funding: 0%; State funding: 0%; County funding: 0%; Realignment funding: 0%; Other funding: 0%	**Budget Adjustment:** No
	For Fiscal Year: 17/18

C.E.O. RECOMMENDATION: Approve.

BACKGROUND:

Summary

The Coordinated Care Initiative (CCI) was created in 2012 in an effort to reduce state costs and improve health care delivery by coordinating services through a single health plan. California Welfare and Institutions Code (W&IC) section 14186.35 required In-Home Supportive Services (IHSS) to be a Medi-Cal benefit available through managed care health plans in seven counties as part of the CCI.

The Legislature's intent was to implement a pilot project of IHSS as a managed care benefit. Piloting counties performed functions necessary for the administration of the IHSS program, including conducting assessments and determining authorized hours for recipients. The W&IC also required managed care health plans administer the program, including entering into a Memorandums of Understanding (MOU) with each county where IHSS was provided as a managed care benefit. Riverside County In-Home Supportive Services-Public Authority entered into agreements with IEHP and Molina, on January 1, 2014, that outlined the overarching duties involved in setting up and maintaining the pilot project.

In fiscal year 2016-2017, the Director of Finance determined the CCI pilot project no longer cost-effective, as reflected in the Governor's 2017-2018 budget. As a result, Senate Bill 97 (approved by the Governor on July 10, 2017) terminated the requirement for IHSS to be a managed care benefit through managed care health plans, effective January 1, 2018.

The Governor's budget also recommended counties and managed care health plans continue partnerships and facilitate coordination of services for mutual clients. The new MOUs between IHSS-PA and IEHP and Molina will allow continued coordination of benefits, sharing confidential recipient information, promoting shared understanding of client needs and appropriate access to programs within the DPSS Adult Services Division.

Impact on Residents and Businesses

In-Home Supportive Services (IHSS) provides qualified aged, blind and disabled person with services that permit them to remain in their own homes and avoid institutionalization.

SUPPLEMENTAL:

SUBMITTAL TO THE RIVERSIDE COUNTY IN-HOME SUPPORTIVE SERVICES PUBLIC AUTHORITY
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

Additional Fiscal Information
There are no financial components to these agreements.

ATTACHMENTS:

PA-03810 – PA and IEHP
PA-03811 – PA and Molina

Jennifer Sargent, Principal Management Analyst 12/5/2017

Tina Grande, Assistant Purchasing Director 11/29/2017

Gregory P. Priamos, Director County Counsel 11/29/2017

Riverside County In-Home Supportive Services Public Authority (PA)
Contracts Administration Unit
10281 Kidd Street
Riverside, CA 92503

OPERATIONAL AGREEMENT:	PA-03810
AGENCY:	Inland Empire Health Plan
AGREEMENT TERM:	January 1, 2018 – December 31, 2022
MAXIMUM REIMBURSABLE AMOUNT:	$0.00

WHEREAS, the Riverside County In-Home Supportive Services Public Authority, hereinafter referred to as PA, desires to enter into an Agreement with Inland Empire Health Plan, hereinafter referred to as "PLAN", to provide for continued coordination of benefits with managed care system;

WHEREAS, Inland Empire Health Plan also desires to provide for continued coordination of benefits with managed care system;

WHEREAS, PA desires Inland Empire Health Plan to perform these services in accordance with the TERMS and CONDITIONS (T&C) attached hereto and incorporated herein by this reference. The T&C specify the responsibilities of PA and Inland Empire Health Plan;

NOW THEREFORE, PA and Inland Empire Health Plan do hereby covenant and agree that Inland Empire Health Plan shall provide said services in accordance with the terms and conditions contained herein of this Agreement.

Authorized Signature for PA	**Authorized Signature for: Inland Empire Health Plan:**
Printed Name of Person Signing: John F. Tavaglione	Printed Name of Person Signing: Rohan Reid, Executive Officer on behalf of: Bradley P. Gilbert
Title: Chair, Board of Supervisors	Title: CEO
Address: 4060 County Circle Dr. Riverside, CA 92503	Address: 10801 Sixth St, Suite 120 Rancho Cucamonga, CA 91730
Date Signed: DEC 12 2017	Date Signed: 11/20/17

ATTEST: KECIA HARPER-IHEM, Clerk
By _____ DEPUTY

FORM APPROVED COUNTY COUNSEL
By _____ 11/29/17
KRISTINE BELL-VALDEZ DATE

DEC 12 2017 7.2

TABLE OF CONTENTS

List of Exhibits

AGREEMENT TERMS AND CONDITIONS

I. DEFINITIONS

A. "APS" refers to Adult Protective Services.

B. "ASD" refers to Adult Services Division, and all programs and staff under ASD, including APS, In-Home Supportive Services (IHSS) Homeless Programs, and Public Authority (PA).

C. "CCT" refers to Coordinated Care Team.

D. "COUNTY" refers to the County of Riverside.

E. "DPSS" refers to the County of Riverside and its Department of Public Social Services, which has administrative responsibility for this MOU.

F. "IHSS" refers to In-Home Supportive Services.

G. "PA" refers to the Riverside County In-Home Supportive Services (IHSS) Public Authority.

II. OBJECTIVES

This MOU gives the PA and PLAN the authority to perform functions in coordination with a managed care system, including but not limited to:

1. Continued coordination of benefits
2. Serving clients collectively
3. Coordinating person-centered approach to service delivery
4. Sharing of confidential recipient information to promote shared understanding of client needs and ensure appropriate access to healthcare.

III. PA RESPONSIBILITIES

A. PA shall initiate contact with PLAN to advocate on behalf of mutual clients.

B. PA shall participate in CCTs as needed for coordination of client services.

C. PA shall enroll IHSS providers, conduct provider orientation, and retain enrollment documentation in the manner set forth in WIC section 12301.24 and 12305.81; as delegated by DPSS and pursuant to WIC section 12301.6.

D. PA shall ensure criminal background checks are conducted by the IHSS Public Authority on all potential providers of IHSS and that providers are excluded consistent with the provisions set forth in WIC sections 12305.81, 12305.86 and 12305.87.

E. PA shall notify PLAN when additional services or emergency backup services are needed. PA and PLAN shall coordinate to provide these services to clients referred, as needed and agreed upon.

F. PA shall provide assistance to IHSS recipients in finding eligible providers through the establishment of a registry as well as provide training for recipients and providers as set

forth in WIC section 12301.6; or may delegate this responsibility to an entity pursuant to WIC section 12300.7.

G. PA shall act as the employer of record and provide access to trained IHSS providers. For the purpose of this MOU, "trained IHSS providers" refers to those IHSS providers who have met the requirements of the All County Letter (ACL) 10-33, ACL 11-12, ACL 11-44, and ACL 06-59.

H. PA shall be deemed to be the employer for IHSS personnel within the meaning of Chapter 10 of Division 4 of Title 1 of the Government Code, until Riverside County has transitioned and this function is taken over by the California In-Home Supportive Services Authority, pursuant to subdivision (a) of Welfare and Institutions Code section 12300.7.

I. PA shall share confidential data necessary to implement the provisions of the MOU.

J. PA shall appoint an advisory committee to be comprised of not more than 11 people, and no less than 50 percent of the membership of the advisory committee shall be individuals who are current or past users of personal assistance paid through public or private funds or recipients of IHSS services.

K. PA shall participate in administrative fair hearings conducted pursuant to WIC section 10950 et seq. by collaborating with ASD administration to determine positions that support the county action and participating in the hearing as a witness where applicable.

L. PA shall designate a contact person to be responsible for oversight and supervision of the terms of this MOU and act as a liaison throughout the term of the MOU. PA shall immediately notify PLAN in writing of a change in the liaison. The contact person at PA shall be:

Jennifer de la Ossa-Ramirez
Riverside County In-Home Supportive Services Public Authority
12125 Day Street, Suite S-101
Moreno Valley, CA 92557
951-321-6168

M. PA will provide training to managed care plan staff, as requested, that may include but is not limited to:
   a. Function of the Public Authority
   b. Eligibility & Assessment criteria of IHSS recipients
   c. Services provided to IHSS recipients
   d. How to review and understand data made available to the plans electronically (e.g. IHSS case management information payroll systems (CMIPS) data)

N. PA may receive confidential recipient information necessary from the PLAN to promote shared understanding of the client's needs and ensure appropriate access to PA programs.

O. PA shall store confidential information received pursuant to this MOU in a place physically secure from access by unauthorized persons.

P. PA shall instruct any employee with access to the confidential information received pursuant to this MOU regarding the confidential nature of the information.

Q. PA agrees to comply with all applicable policies and procedures of PLAN relating to the performance of this MOU, including but not limited to those regarding privacy and security of confidential member information and the provision of managed care benefits to members.

R. PA shall provide information to PLAN as needed or as requested to complete Reporting requirements from the State or management.

IV. PLAN RESPONSIBILITIES

A. PLAN shall share confidential beneficiary information, to the extent that is allowed under applicable law, and data files with PA to promote shared understanding of the client's needs and ensure appropriate access to all programs under ASD.

B. PLAN may receive confidential beneficiary information necessary to implement this MOU and will use such data only for this purpose; this may include information necessary from the PA to promote shared understanding of the consumer's needs and ensure appropriate access to all programs under ASD.

C. PLAN shall store confidential information received pursuant to this MOU in a place physically secure from access by unauthorized persons.

D. PLAN shall instruct any employee with access to the confidential information received pursuant to this MOU regarding the confidential nature of the information.

E. PLAN, in consultation with PA, shall continue the current referral process, care coordination team processes, and other coordination that needs to be enhanced to ensure the appropriate access to healthcare.

F. PLAN shall designate a contact position, with the current employee's name, to be responsible for oversight and supervision of the terms of this MOU and to act as a liaison throughout the term of the MOU. PLAN will immediately notify PA in writing of a change in the liaison. The contract position at PLAN will be:

Roger Uminski
Inland Empire Health Plan
10801 Sixth Street, Suite 120
Rancho Cucamonga, CA 91730
909-296-3579

G. PLAN shall notify PA when additional services or emergency backup services are needed. PLAN and PA shall coordinate to provide these services to clients referred, as needed and agreed upon.

H. PLAN may assist current ASD clients with the completion of an SOC 873, IHSS Health Certification Form, when they are notified by PLAN member or PA that a need exists.

I. PLAN shall participate in CCTs as needed for coordination of clients' services.

J. PLAN shall provide training to PA staff, as requested and as mutually agreed is appropriate, that may include, but not be limited to:

1. Overview of Managed Care Processes, Procedures, Prior Authorization criteria, case Management, Utilization Management, drug formulary, contracted providers and website navigation.

2. Eligibility & Assessment of members
3. Services and benefits provided to members
4. How to review and understand data made available to PA.

K. PLAN shall provide information to PA as needed or as requested to complete Reporting requirements from the State or management.

V. DATA CONFIDENTIALITY, SECURITY and SHARING

A. DATA SECURITY

COUNTY and PLAN agree to comply with WIC section 10850 and any other applicable federal and state laws regarding data security and confidentiality, as they now exist, or may be modified in the future, in both electronic and paper format, including, but not limited to, the Health Insurance Portability and Accountability Act of 1996, as amended, Pub.L.014-91.

B. HEALTH INSURANCE PORTABILITY ACCOUNTABILITY ACT (HIPAA)

Under the Health Insurance Portability and Accountability Act (IHPAA), 42 U.S.C. 1320d et seq. and its 162, and 164 ("Privacy Rule and Security Rule"), the Contractor must comply with the Security Rule as a Business Associate, if under this Agreement, it receives, maintains or transmits any health information in electronic form in connection with a transaction covered by part 162 of Title 45 of the Code of Federal Regulations.

The County and Contractor acknowledge that HIPAA mandates them to comply as business associates in order to safeguard protected health information that may be accessed during the performance of this Agreement. The parties agree to the terms and conditions set forth from the County of Riverside Board of Supervisors Policy No. B-23 and the HIPAA Business Associated Agreement with County of Riverside PA as attached hereto as Exhibit A.

All social service privacy complaints should be referred to:

Department of Public Social Services
HR/Administrative Compliance Services Unit
10281 Kidd Street
Riverside, CA 92503
(951) 358-3030

C. PERSONAL HEALTH INFORMATION (PHI)

COUNTY and PLAN will agree to the roles and responsibilities of the sharing of personal health information (PHI) for the purposes set forth in this agreement.

D. PERSONALLY IDENTIFIABLE INFORMATION (PII)

"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 COUNTY and PLAN 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 COUNTY and PLAN shall not duplicate, disseminate or disclose Medi-Cal PII except as allowed in this Agreement.

The COUNTY and PLAN 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 Exhibit B.

When applicable, the COUNTY and PLAN shall incorporate the relevant provisions of Exhibit A into each subcontract or sub-award to subcontractors.

VI. LEGAL SERVICES

In any action at law or in equity, including an action for declaratory relief, brought to enforce or interpret provisions of this MOU. Each party shall bear its own costs, including attorney's fees.

VII. GENERAL

A. EFFECTIVE PERIOD

This Agreement is effective January 1, 2018 through December 31, 2022 and shall remain in effect unless terminated in accordance to the terms included herein.

B. NOTICES

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

PA: In-Home Supportive Services Public Authority
c/o Contracts Administration Unit
P.O. Box 7789
Riverside, CA 92513

Agency: Inland Empire Health Plan
10801 Sixth Street, Suite 120
Rancho Cucamonga, CA 91730

All notices shall be deemed effective when they are made in writing, addressed as indicated above, and deposited in the United States mail. Any notices, correspondence, reports and/or statements authorized or required by this Agreement, addressed in any other fashion will not be acceptable.

C. DUAL INDEMNIFICATION

PLAN shall indemnify and hold harmless the County of Riverside, its Agencies, Districts, Special Districts and Departments, their respective directors, officers, Board of Supervisors,

elected and appointed officials, employees, agents and representatives (individually and collectively hereinafter referred to as Indemnitees) from any liability whatsoever, based or asserted upon any services of PLAN, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this MOU, including but not limited to property damage, bodily injury, or death or any other element of any kind or nature whatsoever arising from the performance of PLAN, its officers, employees, subcontractors, agents or representatives Indemnitors from this MOU.

With respect to any action or claim subject to indemnification herein by PLAN, PLAN shall, at their sole cost, have the right to use counsel of their own choice 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 PLAN's indemnification to Indemnitees as set forth herein.

COUNTY shall indemnify and hold harmless the PLAN, its Departments, their respective directors, officers, Governing Board, elected and appointed officials, employees, agents and representatives (individually and collectively hereinafter referred to as Indemnitees) from any liability whatsoever, based or asserted upon any services of COUNTY, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this MOU, including but not limited to property damage, bodily injury, or death or any other element of any kind or nature whatsoever arising from the performance of COUNTY, its officers, employees, subcontractors, agents or representatives Indemnitors from this MOU.

With respect to any action or claim subject to indemnification herein by COUNTY, COUNTY shall, at their sole cost, have the right to use counsel of their own choice and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of PLAN; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes PLAN's indemnification to Indemnitees as set forth herein.

D. INDEPENDENT PARTIES

It is understood and agreed that the parties are independent contractors and that no relationship of employer-employee exists between the parties hereto. One party's employees shall not be entitled to any benefits payable to employees of the other party, including, but not limited to, Worker's Compensation benefits. The parties shall not be required to make any deductions for employees of the other party from the compensation payable under the provision of this MOU or any such forthcoming agreement.

As independent contractors, the parties hereby hold each other harmless from any and all claims that may be made against the other based upon any contention by any third party that an employer-employee relationship exists by reason of this MOU. As part of the foregoing indemnity, the parties agree to protect and defend at its own expense, including attorney's fees, the other party, its officers, agents and employees in any legal action based upon any such alleged existence of an employer-employee relationship by reason of this MOU.

PLAN shall not be deemed to be the employer of an individual IHSS provider referred to recipients under WIC section 14186.35 for the purposes of liability due to the negligence or intentional torts of the individual IHSS provider.

E. NON-ASSIGNMENT

The parties shall not assign any interest in this MOU, and shall not transfer any interest in the same, whether by assignment or novation, without the prior written consent of the other party. Any attempt to assign or delegate any interest without written consent of the other party shall be deemed void and of no force or effect.

F. GOVERNING LAW

As it pertains to the administration of this MOU, PLAN shall comply, when applicable, with all rules, regulations, requirements, and directives of the California Department of Social Services, other applicable state agencies, and funding sources which impose duties and regulations upon COUNTY, which are equally applicable and made binding upon PLAN as though made with PLAN directly.

G. JURISDICTION

This MOU shall be construed and interpreted according to the laws of the State of California. Any legal action related to the interpretation or performance of this Contract shall be filed only in the appropriate courts located in the County of Riverside, State of California.

H. MODIFICATION

No addition to or alteration of the terms of this MOU, whether by written or verbal understanding of the parties, their officers, agents, or employees shall be valid unless made in writing and formally approved and executed by both parties.

This MOU may be amended at any time by written, mutual consent of all parties.

I. EXTENSION

This MOU may be extended, upon both parties agreement in writing, before or after the term expires.

J. DISPUTES

Except as otherwise provided in this MOU, any dispute concerning a question of fact arising under this MOU, which is not disposed by this MOU, shall be disposed as follows.

There will be three phases of Dispute Resolution and they are as follows:

1. Phase 1
   This phase of dispute resolution will be called "Phase 1 Informal Resolution", and it will be conducted between the PA liaison and Inland Empire Health Plan liaison using the MOU and other supporting documentation maintaining a level of reason, logic and common sense. Phase 1 must be documented.

2. Phase 2
   This phase of dispute resolution will be called "Phase 2 Formal Resolution", and it will be between the Assistant Director of PA and/or his/her designee(s) and the Director of Inland Empire Health Plan or designee. This incident must be written as a note to file.

3. Phase 3
   This phase of dispute resolution will be called "Phase 3 Formal Dispute Resolution," and will be conducted by the Director of Inland Empire Health Plan and the Director of PA.

K. TERMINATION

1. Termination without cause: This MOU may be terminated by either party without cause following 30 days written notice.
2. Termination with cause: This MOU may be terminated immediately by either party if the terms of this MOU are violated.
3. This MOU will be terminated if the contract between DHCS and the PLAN is terminated.

L. AUTHORITY TO EXECUTE

The individuals executing this MOU on behalf of the Parties each represent and warrant that they have the legal and actual authority to bind the Parties to the terms and conditions of this MOU.

This MOU is not effective until signed by both parties.

This document is the full and complete MOU between PA and PLAN.

M. ENTIRE AGREEMENT

This Agreement constitutes the entire Agreement between the parties hereto with respect to the subject matter hereof, and all prior or contemporaneous Agreements of any kind or nature relating to the same shall be deemed to be merged herein.

Exhibit A

HIPAA Business Associate Addendum to the Agreement

Addendum to Contract

Between the County of Riverside and _____

This HIPAA Business Associate Agreement (the "Addendum") supplements, and is made part of the _____ (the "Underlying Agreement") between the County of Riverside ("County") and _____ ("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 tothe 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 of45 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 extentContractor 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: _____

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 my 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 administrationof 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 atCounty 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.

0. 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 PI I 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 .pov, 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 unauthorizedaccess, use, or disclosure of Medi-Cal PI I, 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 abreach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PI I, 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 PI I isattributable 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 breachof 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 ExchangeSecurity 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 thisAgreement 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.

For the County of Department of
(Signature)
(Name)

For the Department of Health Care Services,
(Date)
(Title)
(Signature) (Date)
(Name) (Title)

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

Riverside County In-Home Supportive Services Public Authority (PA)
Contracts Administration Unit
10281 Kidd Street
Riverside, CA 92503

OPERATIONAL AGREEMENT:	PA-03811
AGENCY:	Molina Healthcare of California Partner Plan Inc
AGREEMENT TERM:	January 1, 2018 – December 31, 2022
MAXIMUM REIMBURSABLE AMOUNT:	$0.00

WHEREAS, the Riverside County In-Home Supportive Services Public Authority, hereinafter referred to as PA, desires to enter into an Agreement with Molina Healthcare of California Partner Plan Inc., hereinafter referred to as "PLAN", to provide for continued coordination of benefits with managed care system;

WHEREAS, Molina Healthcare of California Partner Plan Inc. also desires to provide for continued coordination of benefits with managed care system;

WHEREAS, PA desires Molina Healthcare of California Partner Plan Inc. to perform these services in accordance with the TERMS and CONDITIONS (T&C) attached hereto and incorporated herein by this reference. The T&C specify the responsibilities of PA and Molina Healthcare of California Partner Plan Inc.;

NOW THEREFORE, PA and Molina Healthcare of California Partner Plan Inc. do hereby covenant and agree that Molina Healthcare of California Partner Plan Inc. shall provide said services in accordance with the terms and conditions contained herein of this Agreement.

Authorized Signature for PA	**Authorized Signature for: Molina Healthcare of California Partner Plan Inc.:**
Printed Name of Person Signing: John F. Tavaglione	Printed Name of Person Signing: Deborah Miller
Title: Chair, Board of Supervisors	Title: President
Address: 4060 County Circle Dr. Riverside, CA 92503	Address: 200 Oceangate, Suite 100 Long Beach, CA 90802
Date Signed: DEC 12 2017	Date Signed: 11.22.17

ATTEST: KECIA HARPER-IHEM, Clerk
BY _____ DEPUTY

FORM APPROVED COUNTY COUNSEL
BY _____
KRISTINE BELL-VALDEZ DATE

DEC 12 2017 7.2

TABLE OF CONTENTS

List of Exhibits

AGREEMENT TERMS AND CONDITIONS

I. DEFINITIONS

A. "APS" refers to Adult Protective Services.

B. "ASD" refers to Adult Services Division, and all programs and staff under ASD, including APS, In-Home Supportive Services (IHSS) Homeless Programs, and Public Authority (PA).

C. "CCT" refers to Coordinated Care Team.

D. "COUNTY" refers to the County of Riverside.

E. "DPSS" refers to the County of Riverside and its Department of Public Social Services, which has administrative responsibility for this MOU.

F. "IHSS" refers to In-Home Supportive Services.

G. "PA" refers to the Riverside County In-Home Supportive Services (IHSS) Public Authority.

II. OBJECTIVES

This MOU gives the PA and PLAN the authority to perform functions in coordination with a managed care system, including but not limited to:

1. Continued coordination of benefits
2. Serving clients collectively
3. Coordinating person-centered approach to service delivery
4. Sharing of confidential recipient information to promote shared understanding of client needs and ensure appropriate access to healthcare.

III. PA RESPONSIBILITIES

A. PA shall initiate contact with PLAN to advocate on behalf of mutual clients.

B. PA shall participate in CCTs as needed for coordination of client services.

C. PA shall enroll IHSS providers, conduct provider orientation, and retain enrollment documentation in the manner set forth in WIC section 12301.24 and 12305.81; as delegated by DPSS and pursuant to WIC section 12301.6.

D. PA shall ensure criminal background checks are conducted by the IHSS Public Authority on all potential providers of IHSS and that providers are excluded consistent with the provisions set forth in WIC sections 12305.81, 12305.86 and 12305.87.

E. PA shall notify PLAN when additional services or emergency backup services are needed. PA and PLAN shall coordinate to provide these services to clients referred, as needed and agreed upon.

F. PA shall provide assistance to IHSS recipients in finding eligible providers through the establishment of a registry as well as provide training for recipients and providers as set

forth in WIC section 12301.6; or may delegate this responsibility to an entity pursuant to WIC section 12300.7.

G. PA shall act as the employer of record and provide access to trained IHSS providers. For the purpose of this MOU, "trained IHSS providers" refers to those IHSS providers who have met the requirements of the All County Letter (ACL) 10-33, ACL 11-12, ACL 11-44, and ACL 06-59.

H. PA shall be deemed to be the employer for IHSS personnel within the meaning of Chapter 10 of Division 4 of Title 1 of the Government Code, until Riverside County has transitioned and this function is taken over by the California In-Home Supportive Services Authority, pursuant to subdivision (a) of Welfare and Institutions Code section 12300.7.

I. PA shall share confidential data necessary to implement the provisions of the MOU.

J. PA shall appoint an advisory committee continues to be comprised of not more than 11 people, and no less than 50 percent of the membership of the advisory committee shall be individuals who are current or past users of personal assistance paid through public or private funds or recipients of IHSS services.

K. PA shall participate in administrative fair hearings conducted pursuant to WIC section 10950 et seq. by collaborating with ASD administration to determine positions that support the county action and participating in the hearing as a witness where applicable.

L. PA shall designate a contact person to be responsible for oversight and supervision of the terms of this MOU and act as a liaison throughout the term of the MOU. PA shall immediately notify PLAN in writing of a change in the liaison. The contact person at PA shall be:

Jennifer de la Ossa-Ramirez
Riverside County In-Home Supportive Services Public Authority
12125 Day Street, Suite S-101
Moreno Valley, Ca 92557
951-321-6168

M. PA will provide training to managed care plan staff, as requested, that may include but is not limited to:
   a. Function of the Public Authority
   b. Eligibility & Assessment criteria of IHSS recipients
   c. Services provided to IHSS recipients
   d. How to review and understand data made available to the plans electronically (e.g. IHSS case management information payroll systems (CMIPS) data)

N. PA may receive confidential recipient information necessary from the PLAN to promote shared understanding of the client's needs and ensure appropriate access to PA programs.

O. PA shall store confidential information received pursuant to this MOU in a place physically secure from access by unauthorized persons.

P. PA shall instruct any employee with access to the confidential information received pursuant to this MOU regarding the confidential nature of the information.

Q. PA agrees to comply with all applicable policies and procedures of PLAN relating to the performance of this MOU, including but not limited to those regarding privacy and security of confidential member information and the provision of managed care benefits to members.

R. PA shall provide information to PLAN as needed or as requested to complete Reporting requirements from the State or management.

IV. PLAN RESPONSIBILITIES

A. PLAN shall share confidential beneficiary information, to the extent that is allowed under applicable law, and data files with PA to promote shared understanding of the client's needs and ensure appropriate access to all programs under ASD.

B. PLAN may receive confidential beneficiary information necessary to implement this MOU and will use such data only for this purpose; this may include information necessary from the PA to promote shared understanding of the consumer's needs and ensure appropriate access to all programs under ASD.

C. PLAN shall store confidential information received pursuant to this MOU in a place physically secure from access by unauthorized persons.

D. PLAN shall instruct any employee with access to the confidential information received pursuant to this MOU regarding the confidential nature of the information.

E. PLAN, in consultation with PA, shall continue the current referral process, care coordination team processes, and other coordination that needs to be enhanced to ensure the appropriate access to healthcare.

F. PLAN shall designate a contact position, with the current employee's name, to be responsible for oversight and supervision of the terms of this MOU and to act as a liaison throughout the term of the MOU. PLAN will immediately notify PA in writing of a change in the liaison. The contract position at PLAN will be:

Megan Dankmyer
Molina Healthcare of California Partner Plan Inc.
200 Oceangate, Suite 100
Long Beach, CA
888-562-5442 x 125671

G. PLAN shall notify PA when additional services or emergency backup services are needed. PLAN and PA shall coordinate to provide these services to clients referred, as needed and agreed upon.

H. PLAN may assist current ASD clients with the completion of an SOC 873, IHSS Health Certification Form, when they are notified by PLAN member or PA that a need exists.

I. PLAN shall participate in CCTs as needed for coordination of clients' services.

J. PLAN shall provide training to PA staff, as requested and as mutually agreed is appropriate, that may include, but not be limited to:
   1. Overview of Managed Care Processes, Procedures, Prior Authorization criteria, case Management, Utilization Management, drug formulary, contracted providers and website navigation.

2. Eligibility & Assessment of members
3. Services and benefits provided to members
4. How to review and understand data made available to the PA.

K. PLAN shall provide information to PA as needed or as requested to complete Reporting requirements from the State or management.

V. DATA CONFIDENTIALITY, SECURITY and SHARING

A. DATA SECURITY

COUNTY and PLAN agree to comply with WIC section 10850 and any other applicable federal and state laws regarding data security and confidentiality, as they now exist, or may be modified in the future, in both electronic and paper format, including, but not limited to, the Health Insurance Portability and Accountability Act of 1996, as amended, Pub.L.014-91.

B. HEALTH INSURANCE PORTABILITY ACCOUNTABILITY ACT (HIPAA)

Under the Health Insurance Portability and Accountability Act (IHPAA), 42 U.S.C. 1320d et seq. and its 162, and 164 ("Privacy Rule and Security Rule"), the Contractor must comply with the Security Rule as a Business Associate, if under this Agreement, it receives, maintains or transmits any health information in electronic form in connection with a transaction covered by part 162 of Title 45 of the Code of Federal Regulations.

The County and Contractor acknowledge that HIPAA mandates them to comply as business associates in order to safeguard protected health information that may be accessed during the performance of this Agreement. The parties agree to the terms and conditions set forth from the County of Riverside Board of Supervisors Policy No. B-23 and the HIPAA Business Associated Agreement with County of Riverside PA as attached hereto as Exhibit A.

All social service privacy complaints should be referred to:

Department of Public Social Services
HR/Administrative Compliance Services Unit
10281 Kidd Street
Riverside, CA 92503
(951) 358-3030

C. PERSONAL HEALTH INFORMATION (PHI)

COUNTY and PLAN will agree to the roles and responsibilities of the sharing of personal health information (PHI) for the purposes set forth in this agreement.

D. PERSONALLY IDENTIFIABLE INFORMATION (PII)

"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 COUNTY and PLAN 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 COUNTY and PLAN shall not duplicate, disseminate or disclose Medi-Cal PII except as allowed in this Agreement.

The COUNTY and PLAN 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 Exhibit B.

When applicable, the COUNTY and PLAN shall incorporate the relevant provisions of Exhibit A into each subcontract or sub-award to subcontractors.

VI. LEGAL SERVICES

In any action at law or in equity, including an action for declaratory relief, brought to enforce or interpret provisions of this MOU. Each party shall bear its own costs, including attorney's fees.

VII. GENERAL

A. EFFECTIVE PERIOD

This Agreement is effective January 1, 2018 through December 31, 2022 and shall remain in effect unless terminated in accordance to the terms included herein.

B. NOTICES

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

PA: In-Home Supportive Services Public Authority
c/o Contracts Administration Unit
P.O. Box 7789
Riverside, CA 92513

Agency: Molina Healthcare of California Partner Plan Inc.
200 Oceangate, Suite 100
Long Beach, CA

All notices shall be deemed effective when they are made in writing, addressed as indicated above, and deposited in the United States mail. Any notices, correspondence, reports and/or statements authorized or required by this Agreement, addressed in any other fashion will not be acceptable.

C. DUAL INDEMNIFICATION

PLAN shall indemnify and hold harmless the County of Riverside, its Agencies, Districts, Special Districts and Departments, their respective directors, officers, Board of Supervisors,

elected and appointed officials, employees, agents and representatives (individually and collectively hereinafter referred to as Indemnitees) from any liability whatsoever, based or asserted upon any services of PLAN, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this MOU, including but not limited to property damage, bodily injury, or death or any other element of any kind or nature whatsoever arising from the performance of PLAN, its officers, employees, subcontractors, agents or representatives Indemnitors from this MOU.

With respect to any action or claim subject to indemnification herein by PLAN, PLAN shall, at their sole cost, have the right to use counsel of their own choice 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 PLAN's indemnification to Indemnitees as set forth herein.

COUNTY shall indemnify and hold harmless the PLAN, its Departments, their respective directors, officers, Governing Board, elected and appointed officials, employees, agents and representatives (individually and collectively hereinafter referred to as Indemnitees) from any liability whatsoever, based or asserted upon any services of COUNTY, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this MOU, including but not limited to property damage, bodily injury, or death or any other element of any kind or nature whatsoever arising from the performance of COUNTY, its officers, employees, subcontractors, agents or representatives Indemnitors from this MOU.

With respect to any action or claim subject to indemnification herein by COUNTY, COUNTY shall, at their sole cost, have the right to use counsel of their own choice and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of PLAN; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes PLAN's indemnification to Indemnitees as set forth herein.

D. INDEPENDENT PARTIES

It is understood and agreed that the parties are independent contractors and that no relationship of employer-employee exists between the parties hereto. One party's employees shall not be entitled to any benefits payable to employees of the other party, including, but not limited to, Worker's Compensation benefits. The parties shall not be required to make any deductions for employees of the other party from the compensation payable under the provision of this MOU or any such forthcoming agreement.

As independent contractors, the parties hereby hold each other harmless from any and all claims that may be made against the other based upon any contention by any third party that an employer-employee relationship exists by reason of this MOU. As part of the foregoing indemnity, the parties agree to protect and defend at its own expense, including attorney's fees, the other party, its officers, agents and employees in any legal action based upon any such alleged existence of an employer-employee relationship by reason of this MOU.

PLAN shall not be deemed to be the employer of an individual IHSS provider referred to recipients under WIC section 14186.35 for the purposes of liability due to the negligence or intentional torts of the individual IHSS provider.

E. NON-ASSIGNMENT

The parties shall not assign any interest in this MOU, and shall not transfer any interest in the same, whether by assignment or novation, without the prior written consent of the other party. Any attempt to assign or delegate any interest without written consent of the other party shall be deemed void and of no force or effect.

F. GOVERNING LAW

As it pertains to the administration of this MOU, PLAN shall comply, when applicable, with all rules, regulations, requirements, and directives of the California Department of Social Services, other applicable state agencies, and funding sources which impose duties and regulations upon COUNTY, which are equally applicable and made binding upon PLAN as though made with PLAN directly.

G. JURISDICTION

This MOU shall be construed and interpreted according to the laws of the State of California. Any legal action related to the interpretation or performance of this Contract shall be filed only in the appropriate courts located in the County of Riverside, State of California.

H. MODIFICATION

No addition to or alteration of the terms of this MOU, whether by written or verbal understanding of the parties, their officers, agents, or employees shall be valid unless made in writing and formally approved and executed by both parties.

This MOU may be amended at any time by written, mutual consent of all parties.

I. EXTENSION

This MOU may be extended, upon both parties agreement in writing, before or after the term expires.

J. DISPUTES

Except as otherwise provided in this MOU, any dispute concerning a question of fact arising under this MOU, which is not disposed by this MOU, shall be disposed as follows.

There will be three phases of Dispute Resolution and they are as follows:

1. Phase 1
   This phase of dispute resolution will be called "Phase 1 Informal Resolution", and it will be conducted between the PA liaison and Inland Empire Health Plan liaison using the MOU and other supporting documentation maintaining a level of reason, logic and common sense. Phase 1 must be documented.

2. Phase 2
   This phase of dispute resolution will be called "Phase 2 Formal Resolution", and it will be between the Assistant Director of PA and/or his/her designee(s) and the Director of Inland Empire Health Plan or designee. This incident must be written as a note to file.

3. Phase 3
   This phase of dispute resolution will be called "Phase 3 Formal Dispute Resolution," and will be conducted by the Director of Inland Empire Health Plan and the Director of PA.

K. TERMINATION

1. Termination without cause: This MOU may be terminated by either party without cause following 30 days written notice.
2. Termination with cause: This MOU may be terminated immediately by either party if the terms of this MOU are violated.
3. This MOU will be terminated if the contract between the California Department of Health Care Services (DHCS) and the PLAN is terminated.

L. AUTHORITY TO EXECUTE

The individuals executing this MOU on behalf of the Parties each represent and warrant that they have the legal and actual authority to bind the Parties to the terms and conditions of this MOU.

This MOU is not effective until signed by both parties.

This document is the full and complete MOU between PA and PLAN.

M. ENTIRE AGREEMENT

This Agreement constitutes the entire Agreement between the parties hereto with respect to the subject matter hereof, and all prior or contemporaneous Agreements of any kind or nature relating to the same shall be deemed to be merged herein.

Exhibit A

HIPAA Business Associate Addendum to the Agreement

Addendum to Contract

Between the County of Riverside and _____

This HIPAA Business Associate Agreement (the "Addendum") supplements, and is made part of the _____ (the "Underlying Agreement") between the County of Riverside ("County") and _____ ("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 tothe 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 of45 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 extentContractor 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: _____

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 my 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 administrationof 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 atCounty 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.

0. 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 PI I 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 .pov, 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 unauthorizedaccess, use, or disclosure of Medi-Cal PI I, 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 abreach, security incident, intrusion, or unauthorized access, use, or disclosure of Medi-Cal PI I, 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 PI I isattributable 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 breachof 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 ExchangeSecurity 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 thisAgreement 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.

For the County of Department of
(Signature)
(Name)

For the Department of Health Care Services,
(Date)
(Title)
(Signature) (Date)
(Name) (Title)

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