THE INFORMATION IN THIS BOX IS NOT A PART OF THE CONTRACT AND IS FOR COUNTY USE ONLY

Contract Number

SAP Number

Department of Aging and Adult Service-Public Guardian

Department Contract Representative	Maria Tucci, Contracts Analyst
Telephone Number	(909) 387-2806
Contractor	Riverside County Department of Public Social Services
Contractor Representative	Tracy Chappell Slaughter
Telephone Number	(951) 358-5870
Contract Term	October 1, 2024 through September 30, 2029
Original Contract Amount	Non-Financial
Amendment Amount	
Total Contract Amount	Non-Financial
Cost Center	
Grant Number (if applicable)	N/A

IT IS HEREBY AGREED AS FOLLOWS*:*

WHEREAS, San Bernardino County through its Department of Aging and Adult Services-Public Guardian (DAAS-PG) desires to designate a contractor of choice to provide and obtain Courtesy Investigation of Elder or Dependent Adult Abuse, as further described in a statement of work (the "Services"); and

WHEREAS, based upon and in reliance on the representations of Riverside County Department of Public Social Services (DPSS), the County finds DPSS qualified to provide referrals in situations involving a potential Conflict of Interest; and

WHEREAS, DAAS-PG desires that such services be provided by DPSS and DPSS agrees to perform these services as set forth below;

NOW, THEREFORE, DAAS-PG and DPSS mutually agree to the following terms and conditions:

TABLE OF CONTENTS

A. DEFINITIONS

1. Abuse – The self-neglect, physical abuse, sexual abuse, neglect by others, financial abuse abandonment, isolation, abduction, or other treatment with resulting physical harm, pain, or mental suffering to an elder or dependent adult. Abuse may also include the deprivation by a care custodian of goods or services that are necessary to avoid physical harm or mental suffering.
2. Adult Protective Services (APS) – The preventive and remedial activities performed on behalf of elders and dependent adults who are unable to protect their own interests; harmed or threatened with harm; caused physical or mental injury due to the action or inaction of another person of their own action as a result of ignorance, illiteracy, incompetence, mental limitation, substance abuse, or poor health; lacking in adequate food, shelter, or clothing; exploited of their income and resources; or deprived of entitlement due to them.
3. Assisting County – The county providing the Courtesy Investigation on behalf of the Requesting County (defined below).
4. Conflict of Interest – The allegations of elder or dependent adult abuse or neglect against certain categories of persons identified by each county within its internal policies, including certain county employees, relatives of county employees, or high profile individuals.
5. Courtesy Investigation – An investigation of an elder or dependent adult abuse or neglect report by the Assisting County on behalf of the Requesting County.
6. Department of Aging and Adult Services – Public Guardian (DAAS-PG) – One of eight Departments within San Bernardino County Human Services designated to administer services to the County's well and at risk elder/dependent adult populations. DAAS-PG was formed in 1992 as a result of merging the Department of Adult Services and the Department of Aging.
7. Dependent Adult – A person between the ages of eighteen (18) and fifty-nine (59) years who has physical or mental limitations that restrict his or her ability to carry out normal activities of daily living or to protect his or her rights, including, but not limited to, persons who have physical or developmental disabilities or whose physical or mental abilities have diminished because of age.
8. Department of Public Social Services (DPSS) – The County of Riverside and its Department of Public Social Services, which has administrative responsibility for this contract.
9. Elder(ly) – A person aged sixty (60) years or older, residing within the jurisdiction of the Requesting County or Assisting County in this contract.
10. Interest – A holding prior or future stake, share, or involvement in the undertakings of this contract.
11. Petition – A legal document filed with a court asking the court to open a case when a social worker determines that court intervention is necessary to protect the safety and wellbeing of an elder or dependent adult, which may include probate conservatorship or dependency filing.
12. Requesting County – The county that suspects or has received an initial report of elder or dependent adult abuse or neglect and is requesting the Assisting County to conduct a Courtesy Investigation.
13. Supervising Social Services Practitioner (SSSP) – A highly experienced professional who assigns, guides, and directs the day-to-day activities of the Social Services Practitioner(s) they manage.

B. OBJECTIVES

The objective of this contract between DPSS and DAAS-PG are as follows:

1. To provide and obtain Courtesy Investigations for referrals from DPSS' Adult Services Division and DAAS-PG's Adult Protective Services in situation involving a potential Conflict of Interest; and
2. To identify the responsibilities of each county when serving in the role of the Requesting County or Assisting County when a Courtesy Investigation of Elder or Dependent Adult Abuse or neglect,

as discussed in Welfare and Institutions Code section 15600 et seq., is identified by the Requesting County and the Assisting County agrees to investigate.

C. DPSS RESPONSIBILITIES

DPSS shall:

1. Assign staff to be liaison between DPSS and DAAS-PG.
2. When the County of Riverside is the Requesting County, DPSS will request assistance from DAAS-PG, when necessary, by following the protocol outlined in the chart below:

Stage	Who	Description
1	DPSS APS Central Intake Center Social Worker	If the referral involves a potential Conflict of Interest, notify the Central Intake Center Supervisor.
2	DPSS APS Central Intake Center Supervisor	Consult with the Central Intake Center Regional Manager.
3	DPSS APS Supervising Social Services Practitioner (SSSP)	Request DAAS-PG perform a Courtesy Investigation by contacting the following: DAAS hotline at (877) 565-2020 and speak with DAAS-PG SSSP between the business hours of 8 a.m. - 5 p.m. Monday-Friday. The Child and Adult Abuse Hotline (CAAHL) Supervisor may be contacted during afternoons only Monday - Thursday 5:30 p.m. – 8 a.m., Friday 5 p.m. through Monday 8 a.m., and on holidays.
4	DPSS APS Call Center	Assign the request to a DAAS-PG APS Supervisor at the appropriate region. After consultation, the DAAS-PG APS Supervisor will approve or deny the request for DAAS-PG to conduct the investigation.
5	DPSS APS Call Center	If the DAAS-PG APS Supervisor approves the request, immediately make a report to DAAS-PG Call Center or CAAHL hotline advising that the two counties have conferred, and DAAS-PG has agreed to investigate the referral and follow the steps in the "Courtesy Investigations" section below.
6	DPSS APS Central Intake Center Supervisor	If the DAAS-PG APS Supervisor denies the request, DPSS shall follow its usual procedures for requesting another county to perform the Courtesy Investigation or for investigating the Elder or Dependent Adult Abuse, as appropriate.

D. DAAS-PG RESPONSIBILITIES

DAAS-PG shall:

1. Assign staff to be liaison between DPSS and DAAS-PG.
2. When San Bernardino County is the Requesting County, DAAS-PG will request assistance from DPSS when necessary, by following the protocol outlined in the chart below:

Stage	Who	Description
1	DAAS-PG APS Call Center	Once it has been identified that the referral involves a potential Conflict of Interest, notify the District Manager (DM).
2	DAAS-PG APS Call Center	Consult with the DAAS-PG APS Supervisor.

3	DAAS-PG SSSP	If the DAAS-PG SSSP approves the request, DAAS-PG SSSP will request DPSS perform a Courtesy Investigation by contacting the following: DPSS hotline at (800) 491-7123 and speak with the DPSS APS Supervisor.
4	DAAS-PG SSSP	After the counties have conferred and in agreement of the request, DAAS-PG SSSP will immediately make a report to DPSS hotline advising that the two counties have conferred and DPSS has agreed to investigate the referral and follow the steps in the "Courtesy Investigations" section below.
5	DAAS-PG SSSP	If the DPSS APS Supervisor denies the request, DAAS-PG shall follow its usual procedures for investigating the Elder or Dependent Adult Abuse.

E. COURTESY INVESTIGATIONS

1. If the Assisting County does not agree to perform the Courtesy Investigation, the Assisting County's liaison shall contact the Requesting County's liaison to discuss further before declining the request.

2. If the Assisting County agrees to conduct a Courtesy Investigation pursuant to section C and D above, then the Assisting County shall independently assess the allegation of elder or dependent adult abuse.

   a. The Assisting County will review information already gathered by the Requesting County and/or conduct an independent, new investigation including interviews.

   b. The Assisting County shall determine if the referral requires an immediate or ten (10) day response.

   c. Upon completion of the investigation, the Assisting County shall immediately inform the Assistant Director of Adult Services for the Requesting County of its finding.

   d. Within forty-eight (48) hours of completing the investigation, the Assisting County shall submit a written report to the Requesting County. The report may be the completed SOC 343 – Investigation of Suspected Dependent Adult/Elder Abuse or another report that includes the same information contained in the SOC 343 form.

   e. Notwithstanding section V.B.5.b., the Requesting County is responsible for making the final determination on the case and litigating the case, if necessary.

   f. The Assisting County shall be responsible for all costs related to the Courtesy Investigation, except for costs under section 33-620.1 and 33-620.2 of the Manual of Policies and Procedures for the Adult Protective Services Program.

   g. All Riverside County DPSS employees traveling to San Bernardino County and/or performing work under this contract are still subject to all Riverside County and DPSS program guidelines.

   h. All San Bernardino County DAAS-PG employees traveling to Riverside County and/or performing work under this contract are still subject to all San Bernardino County and DAAS-PG program guidelines.

F. CONFLICT OF INTEREST

DAAS-PG and their employees and agents, DPSS, and their employees and agents shall have no Interest, and shall not acquire any Interest, direct or indirect, which shall conflict in any manner or degree with the performance of services required under this CONTRACT.

G. NON-DISCRIMINATION

1. In the performance of this contract, both Parties agree that they shall not engage nor employ any unlawful discriminatory practices in the admission of clients, provisions of services or benefits, assignment of accommodations, treatment, evaluation, employment of personnel, or in any other respect on the basis of sex, race, color, ethnicity, national origin, ancestry, religion, age, marital status, medical condition, sexual orientation, sexual preference, gender identity or expression, physical or mental disability, or any other protected group in accordance with the requirements of all applicable federal and state laws.
2. Both Parties shall develop an Affirmative Action Program Plan which meets the lawful and applicable requirements of the U.S. Department of Health and Human Services.
3. DPSS shall furnish any and all information requested by DAAS-PG and shall permit DAAS-PG access, during business hours, to books, records, and accounts in order to ascertain DPSS-PG's compliance with Paragraph G.
4. DAAS-PG shall furnish any and all information requested by DPSS and shall permit DPSS access, during business hours, to books, records, and accounts (both electronic/imaged and physical) in order to ascertain DAAS-PG compliance with Paragraph G.

H. CONFIDENTIALITY

DAAS-PG and DPSS agree to maintain confidentiality of all records pursuant to Welfare and Institution Code sections 10850-10853, 15633, and 15633.5, the California Department of Social Services Manual of Policies and Procedures, Division 19-000; and all other provisions of law and regulations promulgated thereunder relating to privacy and confidentiality, as each may now exist or be hereafter amended.

I. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

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

Social service privacy complaints should be referred to:

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

DAAS-PG: Jennifer Lei
Privacy and Security Officer (PSO)
825 E. Hospitality Lane
San Bernardino, CA 92415
(909) 383-9665
HSPrivacySecurityOffice@hss.sbcounty.gov

J. PERSONALLY, IDENTIFIABLE INFORMATION

Personally, Identifiable Information (Pll) refers to personally identifiable information that can be used alone or in conjunction with any other reasonably available information, to identify a specific individual. Pll includes, but is not limited to, an individual's name, social security number, driver's license number, identification number, biometric records, date of birth, place of birth, or mother's maiden name. The Pll may be electronic, paper, verbal, or recorded. PII may be collected performing administrative functions

on behalf of programs, such as determining eligibility for, or enrollment in, and collecting PII for such purposes, to the extent such activities are authorized by law.

DAAS-PG may use or disclose PII only to perform functions, activities or services directly related to the administration of programs in accordance with Welfare and Institutions Code sections 10850 and 14100.2, or 42 Code of Federal Regulations (CFR) section 431.300 et. seq, and 45 CFR 205.50 et. seq, or as required by law. Disclosures which are required by law, such as a court order, or which are made with the explicit written authorization of the client, are allowable. Any other use or disclosure of PII requires the express approval in writing of DPSS. DAAS-PG shall not duplicate, disseminate or disclose PII except as allowed in this CONTRACT.

DASS-PG agrees to the PII Privacy and Security Standards attached as Attachment II. When applicable, DAAS-PG shall incorporate the relevant provisions of Attachment II into each subcontract or sub-award to subcontractors.

L. FISCAL PROVISIONS

This MOU is a non-financial agreement and neither Party to the CONTRACT shall be obligated to pay any monetary compensation to the other. Further, neither Party to this CONTRACT shall be obligated to pay any third party as a result of this CONTRACT.

M. HOLD HARMLESS/INDEMNIFICATION

Pursuant to the provisions of California Government Code section 895 et seq., each Party agrees to defend, indemnify, and hold harmless each other from any liability, claim or judgment for injury or damages caused by a negligent or wrongful act or omission of any agent, officer, and/or employee of the indemnifying Party which occurs or arises out of the performance of this contract. In the event a Party is determined to be comparatively at fault for any claim, action, loss or damage which results from their respective obligations under the contract, that Party shall indemnify the other Party to the extent of its comparative fault.

N. INSURANCE

1. Prior to the provision of services under this contract, both Parties agree to purchase all required insurance, or maintain program of self-insurance, at Parties' expense and to deposit with DAAS-PG and DPSS Certificates of Insurance, including all endorsements required herein, necessary to satisfy both Parties that the insurance provisions of this contract have been complied with, and to keep such insurance coverage and the certificates therefore on deposit with both parties during the entire term of this contract.
2. If either Party fails to maintain insurance acceptable to DAAS-PG and DPSS for the full term of this contract, either Party may terminate this contract.
3. Qualified Insurer:
    a. The policy or polices of insurance required herein must be issued by an insurer with a minimum rating of A- (Secure A.M. Best's Rating) and VIII (Financial Size Category as determined by the most current edition of the Best's Key Rating Guide/Property-Casualty/United States or ambest.com). It is preferred, but not mandatory, that the insurer be licensed to do business in the state of California (California Admitted Carrier).
    b. If the insurance carrier does not have an A.M. Best Rating of A-/VIII, the CEOs/Offices of Risk management for DAAS-PG and DPSS retain the right to approve or reject the other Party's carrier after a review of the company's performance and financial rating.
4. The policy or policies of insurance maintained by both Parties shall provide the minimum limits and coverage as set forth below.

Coverage	Minimum Limits

Commercial General Liability	$1,000,000 per occurrence $2,000,000 aggregate
Automobile Liability including coverage for owned, non-owned, and hired vehicles	$1,000,000 per occurrence
Worker's Compensation	Statutory
Employer's Liability Insurance	$1,000,000 per occurrence
Sexual Misconduct	$1,000,000 per occurrence
Network Security & Privacy Liability	$1,000,000 per occurrence

5. Required Endorsements:

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

      i. An Additional Insured endorsement using ISO form CG 2010 or CG 2033 or a form at least as broad naming the other Party and its elected and appointed officials, officers, employees, and agents as Additional Insureds.

      ii. A primary and noncontributing endorsement evidencing that DPSS's insurance or DAAS's insurance, as applicable, is primary and any insurance or self-insurance maintained by the other Party shall be excess and noncontributing.

   b. The Network Security and Privacy Liability policy shall contain the following endorsements which shall accompany the Certificate of Insurance:

      i. An Additional Insured endorsement naming the other Party and its elected and appointed officials, officers, employees, and agents as Additional Insureds.

      ii. A primary and noncontributing endorsement evidencing that DPSS's insurance or DAAS's insurance, as applicable, is primary and any insurance or self-insurance maintained by the other Party shall be excess and noncontributing.

6. All insurance policies required by this CONTRACT shall waive all rights of subrogation against the other Party and members of its Board of Supervisors, its elected and appointed officials, officers, agents, and employees when acting within the scope of their appointment or employment.

7. The Workers' Compensation policy shall contain a waiver of subrogation endorsement waiving all rights of subrogation against the other Party and its elected and appointed officials, officers, agents, and employees.

8. DAAS-PG and DPSS shall notify the other Party in writing within thirty (30) days of any policy cancellation and within ten (10) days for nonpayment of premium and provide a copy of the cancellation notice to the other Party. Failure to provide written notice of cancellation my constitute a material breach of the contract, upon which DAAS-PG or DPSS, as applicable, may suspend or terminate this contract.

9. The Commercial General Liability policy shall contain a severability of interests clause also known as a "separation of insureds" clause (standard in the ISO CG 0001 policy).

10. Insurance certificates should be mailed to each Party at the address indicated below:

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

    DAAS-PG San Bernardino County Department of Human Services Administration
    Contracts Administration Unit

11. Each Party shall notify the other Party in writing of changes in the insurance requirements. If DAAS-PG or DPSS, as applicable, does not deposit copies of acceptable certificates of insurance and endorsements with the other Party incorporating such changes within thirty (30) days of receipt of such notice, this contract may be in breach without further notice to the breaching Party, and the nonbreaching Party shall be entitled to all legal remedies.

12. The procuring of such required policy or policies of insurance shall not be construed to limit either Party's liability hereunder nor to fulfill the indemnification provisions and requirements of this CONTRACT, nor act in any way to reduce the policy coverage and limits available from the insurer.

13. Proof of self-insurance in an amount to cover all of the above amounts shall be considered appropriate insurance for this section.

O. RECORDS

1. DAAS-PG and DPSS shall prepare and maintain accurate and complete records of clients served and dates and type of services provided under the terms of this contract.

2. All electronic client records related to services provided under the terms of this contract shall be retained permanently by DAAS-PG and DPSS. The assisting county will transfer the electronic files to the requesting county upon request.

P. TERM

This contract is effective on October 1, 2024 and expires on September 30, 2029, but may be terminated earlier in accordance with provisions of Section O of this contract. The Parties to this contract, however, shall be obligated to perform such duties as would normally extend beyond this term, including, but not limited to, obligations with respect to indemnification, reporting, retention of records, and confidentiality.

Q. EARLY TERMINATION

This contract may be terminated without cause upon thirty (30) days written notice by either Party. The DPSS/DAAS-PG Directors are authorized to exercise his/her rights with respect to any termination of this contract. The DPSS/DAAS-PG Director, or his/her appointed designee, has authority to terminate this contract on behalf of his/her agency.

R. GENERAL PROVISIONS

Any alterations, variations, modifications, or waivers of provisions of the CONTRACT, unless specifically allowed in the contract, shall be valid only when they have been reduced to writing duly signed, and approved by the authorized representatives of all Parties as an amendment to this contract. No oral understanding or agreement not incorporated herein shall be binding on any of the Parties hereto.

S. DISPUTES

A. The parties shall attempt to resolve any disputes amicably at the working level. If that is not successful, the dispute shall be referred to the senior management of the parties. Any dispute relating to this Contract which is not resolved by the parties shall be decided by DPSS's Compliance Contract Officer who shall furnish the decision in writing. The decision of DPSS's Compliance Contract Officer shall be final and conclusive unless determined by a court to have been fraudulent, capricious, arbitrary, or so grossly erroneous as necessarily to imply bad faith. DAAS-PG shall proceed diligently with the performance of this Agreement pending resolution of a dispute.

B. Prior to the filing of any legal action related to this Agreement, the parties shall be obligated to attend a mediation session in Riverside County before a neutral third party mediator. A second

mediation session shall be required if the first session is not successful. The parties shall share the cost of the mediations.

T. CONCLUSION

1. This contract, of twenty eight (28) pages, is the full and complete document describing services to be rendered by DPSS and DAAS-PG.
2. The signatures of the Parties affixed to this contract affirm they are duly authorized to commit and bind their respective agency to the terms and conditions set forth in this document.
3. This contract may be executed in any number of counterparts, each of which so executed shall be deemed to be an original, and such counterparts shall together constitute one and the same contract. The parties shall be entitled to sign and transmit an electronic signature of the contract (whether by facsimile, PDF or other email transmission), which signature shall be binding on the party whose name is contained therein. Each party providing an electronic signature agrees to promptly execute and deliver to the other party an original signed contract upon request.

IN WITNESS WHEREOF, San Bernardino County and the Contractor have each caused this Contract to be subscribed by its respective duly authorized officers, on its behalf.

SAN BERNARDINO COUNTY

►

, Chair, Board of Supervisors

Dated:

SIGNED AND CERTIFIED THAT A COPY OF THIS DOCUMENT HAS BEEN DELIVERED TO THE CHAIRMAN OF THE BOARD

Lynna Monell
Clerk of the Board of Supervisors
San Bernardino County

By

Deputy

RIVERSIDE COUNTY
Department of Public Social Services
(Print or type name of corporation, company, contractor, etc.)

By ►

(Authorized signature - sign in blue ink)

Name Charity Douglas
(*Print or type name of person signing contract)*

Title Director, DPSS
(Print or Type)

Dated:

Address 4060 County Circle Dr. Riverside, CA 92503

Approval as to Form
Minh C. Tran
County Counsel

By:
Katherine Wilkins
Deputy County Counsel

Date:

FOR COUNTY USE ONLY

Approved as to Legal Form	Reviewed for Contract Compliance	Reviewed/Approved by Department
►	►	►
Jacqueline Carey-Wilson, Deputy County Counsel	Patty Steven, Contracts Manager	Sharon Nevins, Director
Date	Date	Date

HIPAA Business Associate Agreement
Addendum to Contract
Between the County of Riverside and San Bernardino County Department of Aging and Adult Service – Public Guardian

This HIPAA Business Associate Agreement (the "Addendum") supplements, and is made part of ("Underlying Agreement") between the County of Riverside DPSS and San Bernardino County DAAS-PG and shall be effective as of the date the Underlying Agreement is approved by both Parties (the "Effective Date").

RECITALS

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

WHEREAS, to the extent the Parties discloses PHI and/or ePHI creates, receives, maintains, transmits, or has access to PHI and/or ePHIof the Parties, Each Party 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 as a business associate of the Parties, including the establishment of permitted and required uses and disclosures of PHI and/or ePHI created or received by the Parties during the course of performing functions, services and activities, 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:

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 the Parties 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 the Parties 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).

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

A. Except as otherwise provided in this Addendum, the Parties may use, disclose, or access PHI and/or ePHI as necessary to perform any and all obligations 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), the Parties may:

(1) Use PHI and/or ePHI if necessary for the Party's proper management and administration and to carry out its legal responsibilities; and,

(2) Disclose PHI and/or ePHI for the purpose of the Party's proper management and administration or to carry out its legal responsibilities, only if:

(a) The disclosure is required by law; or,

(b) the Parties obtains reasonable assurances, in writing, from the person to whom the Parties 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 the Parties disclosed it to the person, or as required by law; and,

(ii) Notify the Parties 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 the Parties pursuant to the Underlying Agreement or as requested by the Parties; and,

(4) De-identify all PHI and/or ePHI of the Parties received by the Parties 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.

Prohibited Uses and Disclosures.

A. the Parties 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 the Parties.

B. The Parties may neither use, disclose, nor access PHI and/or ePHI it receives from the Parties or from another business associate of the Parties, except as permitted or required by this Addendum, or as required by law.

C. The Parties agree not to make any disclosure of PHI and/or ePHI that the Parties would be prohibited from making.

D. The Parties 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. The Parties agree:

(1) Not to use or disclose PHI for fundraising, unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.514(f) or 45 CFR §164.508;

(2) Not to use or disclose PHI for marketing, as defined in 45 CFR §164.501, unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.508(a)(3);

(3) Not to disclose PHI, except as otherwise required by law, to a health plan for purposes of carrying out payment or health care operations, if the individual has requested this restriction pursuant to 42 USC §17935(a) and 45 CFR §164.522, and has paid out of pocket in full for the health care item or service to which the PHI solely relates; and,

(4) Not to receive, directly or indirectly, remuneration in exchange for PHI, or engage in any act that would constitute a sale of PHI, as defined in 45 CFR §164.502(a)(5)(ii), unless permitted by the Underlying Agreement and in compliance with the requirements of a valid authorization under 45 CFR §164.508(a)(4). This prohibition shall not apply to payment by the Parties for services provided pursuant to the Underlying Agreement.

Obligations of the Parties.

A. The Parties agree to make its best efforts to notify the Parties promptly in writing of any restrictions on the use or disclosure of PHI and/or ePHI agreed to by the Parties that may affect the Party's ability to perform its obligations under the Underlying Agreement, or this Addendum.

B. The Parties agree to make its best efforts to promptly notify the Parties 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 the Party's ability to perform its obligations under the Underlying Agreement, or this Addendum.

C. The Parties agree to make its best efforts to promptly notify the Parties in writing of any known limitation(s) in its notice of privacy practices to the extent that such limitation may affect the Party's use or disclosure of PHI and/or ePHI.

D. The Parties agree not to request each Party 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. The Parties agree to obtain any authorizations necessary for the use or disclosure of PHI and/or ePHI, so that each Party can perform its obligations under this Addendum and/or Underlying Agreement.

Obligations of the Parties. In connection with the use or disclosure of PHI and/or ePHI, The Parties agree to:

A. Use or disclose PHI only if such use or disclosure complies with each applicable requirement of45 CFR §164.504(e). The Party's 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. The Parties shall promptly notify the Parties if each Party 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 the Parties of a use or disclosure of PHI and/or ePHI by each Party in violation of this Addendum.

E. Report to the Parties 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 the Parties 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 Parties agree through contract to the same restrictions and conditions that apply to the Parties with respect to such PHI and/or ePHI, including the restrictions and conditions pursuant to this Addendum.

G. Make available to the Parties or the Secretary, in the time and manner designated by the Parties or Secretary internal practices, books and records relating to the use, disclosure and privacy protection of PHI received from the Parties, or created or received by the Parties, for purposes of determining, investigating or auditing the Party'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 the Parties), or eligibility of benefits, unless otherwise excepted under 45 CFR §164.508(b)(4) and authorized in writing by the Parties.

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 Parties to the extent that each Party is to carry out obligations under the Privacy Rule.

N. Take reasonable steps to cure or end any pattern of activity or practice of its subcontractor of which the Parties becomes aware that constitute a material breach or violation of the subcontractor's obligations under the business associate contract with the Parties, and if such steps are unsuccessful, The Parties agree to terminate its contract with the subcontractor if feasible.

Access to PHI, Amendment and Disclosure Accounting. The Parties agree to:

A. **Access to PHI, including ePHI.** Provide access to PHI, including ePHI if maintained electronically, in a designated record set to the Parties or an individual as directed by the Parties, within five (5) days of request from the Parties, 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 the Parties directs or agrees to at the request of an individual, within fifteen (15) days of receiving a written request from the Parties, in accordance with 45 CFR §164.526.

C. **Accounting of disclosures of PHI and electronic health record.** Assist the Parties 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 the Parties uses or maintains electronic health records. The Parties shall:

(1) Document such disclosures of PHI and/or electronic health records, and information related to such disclosures, as would be required for the Parties 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 the Parties, provide to the Parties or any individual as directed by the Parties information collected in accordance with this section to permit the Parties to respond to a request by an individual for an accounting of disclosures of PHI and/or electronic health record.

(3) Make available for the Parties 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.

Security of ePHI. In the event the Parties discloses ePHI to the Parties needs to create, receive, maintain, transmit or have access to the Parties ePHI, in accordance with 42 USC §17931 and 45 CFR §164.314(a)(2)(i), and §164.306, The Parties 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 the Parties creates, receives, maintains, or transmits on behalf of the Parties 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 the Party'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 the Parties 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 the Parties any security incident of which the Parties become 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.

Breach of Unsecured PHI. In the case of breach of unsecured PHI, the Parties 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, the Parties shall notify each Party 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 the Parties as of the first day on which such breach is known to the Parties or, by exercising reasonable diligence, would have been known to the Parties, which includes any person, other than the person committing the breach, who is an employee, officer, or other agent of the Parties (determined in accordance with the federal common law of agency).

(2) **Content of notification.** The written notification to the Parties relating to breach of unsecured PHI shall include, to the extent possible, the following information if known (or can be reasonably obtained) by the Parties:

(a) The identification of each individual whose unsecured PHI has been, or is reasonably believed by the Parties 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 the Parties 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 the Parties, the Parties shall cooperate with each Party and shall provide the Parties with any information requested by the Parties to enable the Parties 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, the Parties shall maintain a log or other documentation of such breaches and provide such log or other documentation on an annual basis to the Parties 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 the Party 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, the Parties 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 Party'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, the Parties agree 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 the Party's obligations to indemnify, defend and hold harmless the Parties under Section 9 of this Addendum.

F. **Documentation.** Pursuant to 45 CFR §164.414(b), in the event the Party's use or disclosure of PHI and/or ePHI violates the Privacy Rule, the Parties shall maintain documentation sufficient to demonstrate that all notifications were made by the Parties as required by 45 CFR Part 164, Subpart D, or that such use or disclosure did not constitute a breach, including Party'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 the Parties, 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) The Parties agree to assist the Parties 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) The Parties agree to report to the Parties 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 the Parties detects such incident. The Parties further agree 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.

Hold Harmless/Indemnification.

A. The Parties agree 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 the Parties, 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 the Parties, its officers, agents, employees, subcontractors, agents or representatives from this Addendum. The Parties 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 the Parties, 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 the Parties, the Parties shall, at their sole cost, have the right to use counsel of their choice, subject to the approval of the Parties, 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 the Parties; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes the Party's indemnification to the Parties as set forth herein. The Party's obligation to defend, indemnify and hold harmless the Parties shall be subject to the Parties having given the Parties 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 the Party's expense, for the defense or settlement thereof. The Party's obligation hereunder shall be satisfied when the Parties has provided to the Parties the appropriate form of dismissal relieving the Parties 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 the Party's obligations to indemnify and hold harmless eah Parties 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 Parties from indemnifying each Party 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.

Term. This Addendum shall commence upon the Effective Date and shall terminate when all PHI and/or ePHI provided by the Parties, or created or received by the Parties, is destroyed or returned to the Parties, 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.

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, the Parties shall return or, if agreed to in writing by the Parties, destroy all PHI and/or ePHI received from the Parties, or created or received by the Parties, and, in the event of destruction, the Parties shall certify such destruction, in writing, to each Party. This provision shall apply to all PHI and/or ePHI which are in the possession of subcontractors or agents of the Parties. The Parties shall retain no copies of PHI and/or ePHI, except as provided below in paragraph (2) of this section.

(2) In the event that the Parties determines that returning or destroying the PHI and/or ePHI is not feasible, the Parties shall provide written notification to each Party of the conditions that make such return or destruction not feasible. Upon determination by the Parties that return or destruction of PHI and/or ePHI is not feasible, the Parties 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 the Parties maintains such PHI and/or ePHI.

General Provisions.

A. **Retention Period.** Whenever the Parties is required to document or maintain documentation pursuant to the terms of this Addendum, the Parties 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 the Parties to comply with HITECH, the Privacy Rule, Security Rule, and HIPAA generally.

C. **Survival.** The obligations of the Parties 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 the Parties pursuant to the terms of this Addendum shall be made in writing and delivered to the Parties 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 the Parties may hereafter designate. All notices to the Parties provided by the Parties pursuant to this Section shall be deemed given or made when received by the Parties.

County HIPAA Privacy Officer: HIPAA Privacy Manager

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

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

— — ——— — ——— — TO BE COMPLETED BY COUNTY PERSONNEL ONLY— — ——— ——— —

County Departmental Officer: _____

County Departmental Officer Title: _____

County Department Address: _____

County Department Fax Number: _____

I. PHYSICAL SECURITY

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

A. Secure all areas of the Contractor facilities where staff assist in the administration of their program and use, disclose, or store Pll.

B. These areas shall be restricted to only allow access to authorized individuals by using one or more of the following:
   1. Properly coded key cards
   2. Authorized door keys
   3. Official identification

C. Issue identification badges to Contractor staff.

D. Require Contractor staff to wear these badges where Pll is used, disclosed, or stored.

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

F. Ensure there are security guards or a monitored alarm system at all times at the Contractor facilities and leased facilities where five hundred (500) or more individually identifiable records of Pll is used, disclosed, or stored. Video surveillance systems are recommended.

G. Ensure data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter security and physical access controls that limit access to only authorized staff. Visitors to the data center area must be escorted at all times by authorized staff.

H. Store paper records with PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which are multi-use meaning that there are County and non-County functions in one building in work areas that are not securely segregated from each other. It is recommended that all PII be locked up when unattended at any time, not just within multi-use facilities.

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

II. TECHNICAL SECURITY CONTROLS

A. Workstation/Laptop Encryption. All workstations and laptops, which use, store and/or process PII, must be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.

B. Server Security. Servers containing unencrypted PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

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

D. Mobile Device and Removable Media. All electronic files, which contain PII data, must be encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.

E. Antivirus Software. All workstations, laptops and other systems, which process and/or store PII, must install and actively use an antivirus software solution. Antivirus software should have automatic updates for definitions scheduled at least daily.

F. Patch Management.
   1. All workstations, laptops and other systems, which process and/or store PII, must have critical security patches applied, with system reboot if necessary.
   2. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.
   3. At a maximum, all applicable patches deemed as critical must be installed within thirty (30) days of vendor release. It is recommended that critical patches which are high risk be installed within seven (7) days.
   4. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.

G. User IDs and Password Controls.
   1. All users must be issued a unique user name for accessing PII.
   2. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee within twenty- four (24) hours. Note: Twenty-four (24) hours is defined as one (1) working day.
   3. Passwords are not to be shared.
   4. Passwords must be at least eight (8) characters.
   5. Passwords must be a non-dictionary word.
   6. Passwords must not be stored in readable format on the computer or server.
   7. Passwords must be changed every ninety (90) days or less. It is recommended that passwords be required to be changed every sixty (60) days or less.
   8. Passwords must be changed if revealed or compromised.
   9. Passwords must be composed of characters from at least three (3) of the following four (4) groups from the standard keyboard:
      a. Upper case letters (A-Z)
      b. Lower case letters (a-z)
      c. Arabic numerals (0-9)
      d. Special characters (!,@,#, etc.)

H. Data Destruction. When no longer needed, all PII must be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the PII cannot be retrieved.

I. System Timeout. The systems providing access to PII must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.

J. Warning Banners. The systems providing access to PII must display a warning banner stating, at a minimum:
   1. Data is confidential;
   2. Systems are logged;

3. System use is for business purposes only, by authorized users; and
4. Users shall log off the system immediately if they do not agree with these requirements.

K. System Logging.
   1. The systems which provide access to PII must maintain an automated audit trail that can identify the user or system process which initiates a request for PII, or alters PII.
   2. The audit trail shall:
      a. Be date and time stamped;
      b. Log both successful and failed accesses;
      c. Be read-access only; and
      d. Be restricted to authorized users.
      3. If PII is stored in a database, database logging functionality shall be enabled.
      4. Audit trail data shall be archived for at least three (3) years from the occurrence.

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

M. Transmission Encryption.
   1. All data transmissions of PII outside of a secure internal network must be encrypted using a Federal Information Processing Standard (FIPS) 140-2 certified algorithm that is 128 bit or higher, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS). It is encouraged, when available and when feasible, that 256 bit encryption be used.
   2. Encryption can be end to end at the network level, or the data files containing PII can be encrypted.
   3. This requirement pertains to any type of PII in motion such as website access, file transfer, and email.

N. Intrusion Prevention. All systems involved in accessing, storing, transporting, and protecting PII, which are accessible through the Internet, must be protected by an intrusion detection and prevention solution.

III. AUDIT CONTROLS

A. System Security Review.
   1. The Contractor must ensure audit control mechanisms are in place.
   2. All systems processing and/or storing PII must have at least an annual system risk assessment/security review that ensures administrative, physical, and technical controls are functioning effectively and provide an adequate level of protection.
   3. Reviews should include vulnerability scanning tools.

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

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

IV. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

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

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

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

V. PAPER DOCUMENT CONTROLS

A. Supervision of Data. The PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information.

B. Data in Vehicles. The Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which staff can transport PII, as well as the physical security requirements during transport. A Contractor that chooses to permit its staff to leave records unattended in vehicles must include provisions in its policies to ensure the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.

C. Public Modes of Transportation. The PII in paper form shall not be left unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.

D. Escorting Visitors. Visitors to areas where PII is contained shall be escorted, and PII shall be kept out of sight while visitors are in the area.

E. Confidential Destruction. PII must be disposed of through confidential means, such as cross cut shredding or pulverizing.

F. Removal of Data. The PII must not be removed from the premises except for identified routine business purposes or with express written permission of the County.

G. Faxing.
   1. Faxes containing PII shall not be left unattended and fax machines shall be in secure areas.
   2. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.
   3. Fax numbers shall be verified with the intended recipient before sending the fax.

H. Mailing.
   1. Mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.
   2. Mailings that include five hundred (500) or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt, unless the Contractor obtains prior written permission from the County to use another method.

VI. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

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

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

Breaches should be referred to:

DPSS Privacy Officer
Assurance and Review Services
Riverside County Department of Public Social Services
10281 Kidd Street
Riverside, CA 92503
privacyincident@rivco.org