IHSS PUBLIC AUTHORITY MEMORANDUM OF UNDERSTANDING

COVER PAGE

Memorandum of Understanding between Molina Healthcare of California and County of Riverside on behalf of Public Authority In-Home Supportive Services

DPSS-0005261

This Memorandum of Understanding ("MOU") is entered into by Molina Healthcare of California, ("MCP") and County of Riverside, a political subdivision of the state of California on behalf of Public Authority ("County") regarding In-Home Supportive Services members, effective upon execution ("Effective Date"). County and MCP are referred to herein as a "Party" and collectively as "Parties."

WHEREAS, MCP is required under the Medi-Cal Managed Care Contract, Attachment III, to enter into this MOU, a binding and enforceable contractual agreement, to ensure that Medi-Cal beneficiaries enrolled, or eligible to enroll, in MCP and who are receiving, or are potentially eligible to receive, In-Home Supportive Services Public Authority ("IHSS-PA") ("Members") are able to access and/or receive IHSS services in a coordinated manner from MCP and County; and

WHEREAS, COUNTY is qualified to provide IHSS to MCP Members; and,

WHEREAS, the Parties desire to ensure that Members receive IHSS-PA in a timely manner pursuant to existing State requirements, and that IHSS-PA is coordinated with medical services and long-term services and supports ("LTSS") to promote the health and safety of Members.

In consideration of the mutual agreements and promises hereinafter, the Parties agree as follows:

1. Definitions. Capitalized terms have the meaning ascribed by MCP's Medi-Cal Managed Care Contract with the California Department of Health Care Services ("DHCS"), unless otherwise defined herein. The Medi-Cal Managed Care Contract is available on the DHCS webpage at www.dhcs.ca.gov.

a. "IHSS" refers to In-Home Supportive Services Medi-Cal program that provides in-home assistance to eligible individuals, including children in accordance with Welfare and Institutions Code §12300 *et seq*.

b. "MCP Responsible Person" means the person designated by MCP to oversee MCP coordination and communication with County and ensure MCP's compliance with this MOU as described in Section 4 of this MOU. Pursuant to the DHCS FAQ (12/20/23) this The "MCP Responsible Person" is the person designated by the MCP who is responsible for overseeing the care coordination activities and communications with the Third Party Entity and ensuring the MCP's compliance with the MOU. The MCP Responsible Person is responsible for ensuring the following:

o Meeting at least quarterly with the Third Party Entity to address any issues arising under the MOU;

o Reporting on the MCP's compliance with the MOU to MCP's compliance officer;

o Ensuring there is sufficient staff at MCP to support compliance with and management of the MOU; and

o Serving as, or designating another person to serve as, the point of contact and liaison with the Third Party Entity to ensure the Parties meet regularly, maintain channels of communication, etc.

c. "MCP IHSS-PA Liaison" means MCP's designated point of contact responsible for acting as the liaison between MCP and County as described in Section 4 of this MOU. The MCP-IHSS-PA Liaison must ensure the appropriate communication and care coordination are ongoing between the Parties, facilitate quarterly meetings in accordance with Section 9 of this MOU, and provide updates to the MCP Responsible Person and/or MCP compliance officer as appropriate.

d. "LTSS Liaison" means the person or persons designated by the MCP to provide assistance to support care coordination and transitions from institutional settings as defined by All Plan Letter 23-004 or any subsequent guidance.

e. "IHSS-PA Responsible Person" means the person designated by County to oversee coordination and communication with MCP and ensure County's compliance with this MOU as described in Section 5 of this MOU.

f. "IHSS-PA Liaison" means County's designated point of contact responsible for acting as the liaison between MCP and County as described in Section 5 of this MOU. The IHSS-PA Liaison should ensure the appropriate communication and care coordination are ongoing between the Parties, facilitate, collaborate and participate in quarterly meetings in accordance with Section 9 of this MOU, and provide updates to the IHSS-PA Responsible Person as appropriate.

g. "Multi-disciplinary team" or "MDT" means any team of two or more persons who are trained in the prevention, identification, management, or treatment of abuse of elderly or dependent adults and are qualified to provide a broad range of services related to abuse of elderly or dependent adults, and is defined in Welfare and Institutions Code (WIC) Section 15610.55 et seq. and WIC 10850.1). The MDT is typically facilitated and coordinated by staff of the Adult Protective Services (APS) program, as defined by WIC 15751, and may include other county programs and services to support the elder or dependent adult to create and implement a safety plan for ongoing supports and services.

2. Term. This MOU is in effect as of the Effective Date and continues for a term of five years or as amended in accordance with Section 14.f of this MOU.

3. Services Covered by this MOU. This MOU governs the coordination of care between County and MCP for Members who may be eligible for and/or are receiving IHSS-PA.

4. MCP Obligations.

a. **Provision of Covered Services.** MCP is responsible for authorizing Medically Necessary Covered Services and coordinating care for Members provided by MCP's Network Providers, providing information necessary to assist Members or their Authorized Representatives in referring themselves to County for IHSS-PA, and

coordinating services and other related Medi-Cal LTSS provided by MCP and other providers of carve-out programs, services, and benefits.

i. MCP shall share it's Enhanced Care Management and Community Supports network with the county's network for aging and older adult services to promote alignment.

b. **Oversight Responsibility.** The Director, Healthcare Services, the designated MCP Responsible Person listed in Exhibit A of this MOU, is responsible for overseeing MCP's compliance with this MOU. The MCP Responsible Person must:

i. Meet at least quarterly with County, as required by Section 9 of this MOU;

ii. Report on MCP's compliance with the MOU to MCP's compliance officer no less frequently than quarterly. MCP's compliance officer is responsible for MOU compliance oversight reports as part of MCP's compliance program and must address any compliance deficiencies in accordance with MCP's compliance program policies;

iii. Ensure there is sufficient staff at MCP to support compliance with and management of this MOU;

iv. Ensure the appropriate levels of MCP leadership (i.e., persons with decision-making authority) are involved in implementation and oversight of the MOU engagements and ensure the appropriate levels of leadership from County are invited to participate in the MOU engagements, as appropriate;

v. Ensure training and education regarding MOU provisions are conducted annually for MCP's employees responsible for carrying out activities under this MOU, and as applicable for Subcontractors, Downstream Subcontractors, and Network Providers;

vi. Designate the person or persons at the MCP to serve as the MCP-Long Term Services and Supports ("LTSS") Liaison pursuant to APL 23-004; and while the LTSS Liaison can be the same as the IHSS-PA MCP Liaison, their functions are very different;

vii. Serve, or may designate a person at MCP to serve, as the MCP IHSS-PA Liaison, the point of contact and liaison with County. The MCP-IHSS-PA Liaison is listed in Exhibit A of this MOU. The MCP-IHSS-PA Liaison functions may be assigned to the MCP-LTSS Liaison as long as the MCP-LTSS Liaison meets the training requirements and has the expertise to work with the IHSS-PA Responsible Person, in accordance with DHCS All-Plan Letter ("APL") 23-004 or any subsequent version of the APL and Section 6 of this MOU. MCP must notify County of any changes to the MCP-IHSS-PA Liaison in writing as soon as reasonably practical but no later than the date of change and must notify DHCS within five Working Days of the change; and

viii. Only to the extent that the MCP is able to, designate the person or persons at the MCP to participate in any multidisciplinary team meetings upon the request of the county. Training for participation in and coordination of multidisciplinary team meetings shall facilitated by the county with the MCP.

c. **Compliance by Subcontractors, Downstream Subcontractors, and Network Providers.** MCP must require and ensure that its Subcontractors, Downstream Subcontractors, and Network Providers, as applicable, comply with all applicable provisions of this MOU.

5. County Obligations.

a. **Provision of Services.** Upon receiving the referral from MCP, County is responsible for assessing, approving, and authorizing each Member's initial and continuing need for IHSS-PA pursuant to California Welfare and Institutions Code Section 12300 *et seq*.

b. **Oversight Responsibility.** The Program Specialist, IHSS-PA Responsible Person listed in Exhibit B of this MOU, is responsible for overseeing County's compliance with this MOU. The IHSS-PA Responsible Person serves, or may designate a person to serve, as the designated IHSS-PA Liaison, the point of contact and liaison with MCP. The IHSS-PA Liaison is listed in Exhibit B of this MOU. County must notify MCP of changes to the IHSS-PA Liaison as soon as reasonably practical but no later than the date of change. The IHSS-PA Responsible Person shall review and provide input in the development of any training and education regarding MOU for employees, Subcontractors, Downstream Subcontractors, and Network Providers, as applicable.

6. Training and Education.

a. To ensure compliance with this MOU, MCP must provide training and orientation for County and its employees who carry out responsibilities under this MOU and, as applicable, for MCP's Network Providers, Subcontractors, and Downstream Subcontractors who assist MCP with carrying out MCP's responsibilities under this MOU. The training must include information on MOU requirements, what services are provided or arranged for by each Party, and the policies and procedures outlined in this MOU. For persons or entities performing these responsibilities as of the Effective Date, MCP must provide this training within 60 Working Days of the Effective Date. Thereafter, MCP must provide this training prior to any such person or entity performing responsibilities under this MOU and to all such persons or entities at least annually thereafter. MCP must require its Subcontractors and Downstream Subcontractors to provide training on relevant MOU requirements and County IHSS-PA to its Network Providers.

b. In accordance with health education standards required by the Medi-Cal Managed Care Contract, MCP must provide County, Members, and Network Providers with educational materials related to accessing Covered Services, including for services provided by County. MCP must seek input from the IHSS-PA Liaison in the development of any informational or educational materials and these must meet the cultural and linguistic standards.

c. MCP must provide County, Members, and Network Providers with training and/or educational materials on how MCP's Covered Services and any carved-out services may be accessed, including during nonbusiness hours.

d. MCP, in collaboration with County, must ensure that the MCP-IHSS-PA Liaison is sufficiently trained on IHSS-PA assessment and referral processes and providers, and on how MCP and Primary Care Providers can support IHSS-PA eligibility applications and coordinate care across IHSS-PA, medical services, and LTSS. This includes training on IHSS-PA referrals for Members in inpatient and Skilled Nursing Facility ("SNF") settings as a part of Transitional Care Service requirements, to support safe and stable transitions to home and community-based settings.

e. County may provide its county social workers and other staff with training and educational materials on MCP's Covered Services, including nonemergency medical transportation and nonmedical transportation, to support IHSS-PA consumers and their care providers in assisting Members with accessing MCP's Covered Services.

7. Referrals.

a. **Referral Process.** The Parties must work collaboratively to develop policies and procedures that ensure Members are referred to County for IHSS-PA and/or MCP for the appropriate services.

b. For Members who may be eligible to receive IHSS-PA, who desire IHSS-PA but are not currently receiving IHSS-PA, MCP must submit Member referrals to County using a patient-centered, shared decision-making process.

c. If MCP learns that a Member who is currently receiving IHSS-PA has a condition that has changed, MCP must advise that Member to contact the County IHSS-PA Office to conduct an eligibility redetermination for IHSS-PA.

d. County should refer Members to MCP for MCP's Covered Services, as well as any Community Supports services or care management programs for which Members may qualify, such as Enhanced Care Management ("ECM") or Complex Case Management ("CCM"). MCP shall provide the IHSS-PA-Liaison information regarding its process for screening and accepting referrals and shall provide a written list of ECM and any Community Support services and instructions for referrals to the IHSS-PA-Liaison that can be shared with county staff. However, if County is also an ECM Provider pursuant to a separate agreement between MCP and County for ECM services, this MOU does not govern County's provision of ECM services.

e. If County is notified by an MCP representative that an existing IHSS-PA Member has had a change of condition, County must follow up to determine if a reassessment of IHSS-PA is needed.

Closed Loop Referrals. By January 1, 2025, the Parties must develop a process to implement DHCS guidance regarding closed loop referrals to applicable Community Supports, ECM benefits, and/or community-based resources, as referenced in the CalAIM Population Health Management Policy Guide,[1] DHCS APL 22-024, or any subsequent version of the APL, and as set forth by DHCS through an APL or other, similar guidance. The Parties must work collaboratively to develop and implement a process to ensure that MCP and County comply with the applicable provisions of closed loop referrals guidance within 90 Working Days of issuance of this guidance. The Parties must establish a system that tracks cross-system referrals and meets all requirements as set forth by DHCS through an APL or other, similar guidance.

8. Care Coordination and Collaboration.

a. **Care Coordination.**

i. The Parties must adopt policies and procedures for coordinating Members' access to care and services that incorporate all the requirements set forth in this MOU.

ii. The MCP Responsible Person shall oversee the care coordination activities and communications and shall identify any care coordination issues to be communicated to the County IHSS-PA Responsible Person.

[1] CalAIM Population Health Management Policy Guide, available at https://www.dhcs.ca.gov/CalAIM/Documents/2023-PHM-Policy-Guide.pdf.

iii. The Parties must discuss and address individual care coordination issues or barriers to care coordination efforts at least quarterly.

iv. MCP must have policies and procedures in place to maintain collaboration with County and to identify strategies to monitor and assess the effectiveness of this MOU.

v. MCP's policies and procedures must include:

1. Processes for coordinating with County that ensure there is no duplication of services for Members enrolled in ECM, Community Supports, and other Covered Services through IHSS-PA and that services (such as ECM, Community Supports, and IHSS-PA) are provided in a coordinated and complementary manner. IHSS-PA eligibility does not preclude eligibility for ECM and Community Supports;
2. Processes for ensuring the continuation of Basic Population Health Management and care coordination of all Medi-Cal benefits to be provided or arranged for by MCP while Members receive IHSS-PA; and
3. Processes for outreach and coordination with County (and, to the extent possible, Members and IHSS-PA) for Members identified by DHCS as receiving IHSS-PA.

vi. MCP must assess Members transferring from one care setting or level of care to another, such as from a hospital or an SNF to the home or community, and provide IHSS-PA referral information to Members as appropriate and supporting documentation to County if Members or their Authorized Representatives self-refer to IHSS-PA, as appropriate, as a part of Transitional Care Service requirements in accordance with All County Letter No.: 02-68, All-County Information Notice No.: I-43-06, or any subsequent or superseding guidance.

vii. County should provide Members and their Authorized Representatives, with approval of Members, and IHSS-PA, with information on how to assist Members with obtaining MCP's Covered Services, including any Community Supports or care management programs for which they may qualify, such as ECM or CCM. MCP shall provide informing materials to the County to accomplish this objective for use by county social workers and other appropriate county staff.

viii. The Parties shall develop policies and procedures for coordinating any Enhanced Care Management (ECM) and Community Supports that may enable Members to remain safely in their own homes and communities and avoid hospitalization, SNF or other acute care or institutional care settings, including continuity of care when the Member moves to a different MCP catchment area.

ix. The Parties shall develop policies and procedures for participation in multidisciplinary team meetings, including participation of ECM case managers, LTSS-Liaison, and others as deemed necessary.

9. Quarterly Meetings.

a. The Parties must meet as frequently as necessary to ensure proper oversight of this MOU, but not less frequently than quarterly, in order to address care coordination, Quality Improvement ("QI") activities, QI outcomes, systemic and case specific concerns,

and communication with others within their organizations about such activities. These meetings may be conducted virtually. The length and frequency of such meetings shall be mutually agreed upon by both parties.

b. Within 30 Working Days after each quarterly meeting, MCP must post on its website the date and time the quarterly meeting occurred and, as applicable, distribute to meeting participants a summary of any follow-up action items or changes to processes that are necessary to fulfill MCP's obligations under the Medi-Cal Managed Care Contract and this MOU.

c. MCP must invite the IHSS-PA Responsible Person and appropriate IHSS-PA program executives to participate in MCP quarterly meetings to ensure appropriate committee representation, including a local presence, and to discuss and address care coordination and MOU-related issues. Subcontractors and Downstream Subcontractors should be permitted to participate in these meetings, as appropriate.

d. MCP must report to DHCS updates from quarterly meetings in a manner and at a frequency specified by DHCS and shall provide copies of these updates to the County IHSS-PA Liaison.

e. **Local Representation.** MCP must participate, as appropriate, in meetings or engagements to which MCP is invited by County, such as local county meetings, local community forums, and County engagements, to collaborate with County in equity strategy and wellness and prevention activities.

10. Quality Improvement. The Parties must develop QI activities specifically for the oversight of the requirements of this MOU, including, without limitation, any applicable performance measures and QI initiatives, including those to prevent duplication of services, as well as reports that track referrals, Member engagement, and service utilization. MCP must document these QI activities in its policies and procedures. These Quality Improvement activities shall be articulated in policies and procedures developed by the MCP with input from the IHSS-PA Responsible person and shall be consistent with the DHCS FAQs which state:

"The QI provisions in the MOU Templates are intended to encourage the parties to develop and document activities for how they will assess whether the MOU is improving care coordination and whole-person care and to develop mechanisms to evaluate whether the MOU is effective in achieving its goals. The Parties must develop QI activities specifically for the oversight of the MOU requirements, including, without limitation, any applicable performance measures, and QI initiatives, including those to prevent duplication of services, as well as reports that track referrals, Member engagement, and service utilization. The MCP must document these QI activities in its policies and procedures. MOU QI does not need to meet the QI regulations governing MCPs and/or QI regulations governing specific Third Party Entities." Any data required from the County to meet these requirements will be contingent upon the availability of such data from the State Case Management, Information and Payrolling System (CMIPS) or other data provided by the State.

11. Data Sharing and Confidentiality. The Parties must implement policies and procedures to ensure that the minimum necessary Member information and data for accomplishing the goals of this MOU are exchanged timely and maintained securely and confidentially and in compliance with the requirements set forth below. The Parties must

share information in compliance with the requirements set forth below. Parties shall share Confidential Data of mutual customers of IHSS pursuant to Welfare and Institutions Code sections 14100.2 14005.35, 14005.36, 14005.37 and 22 Cal. Code Regs. § 51009.

a. PROTECTED HEALTH INFORMATION ("PHI").

In the event that there is PHI shared between the Parties pursuant this MOU, the Parties are subject to all relevant requirements contained in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), codified at Title 45, C.F.R., Parts 160 and 164, the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009 (HITECH), Public Law 111-5, enacted February 17, 2009, and the laws and regulations promulgated subsequent hereto and as amended, for purposes of services rendered pursuant to the MOU. The Parties agree to cooperate in accordance with the terms and intent of this MOU for implementation of relevant law(s) and/or regulation(s) promulgated under HIPAA and HITECH. The Parties further agree that it shall be in compliance with the requirements of HIPAA, HITECH, and the laws and regulations promulgated subsequent hereto and as amended. MCP further agrees to the provisions of the HIPAA Business Associate Agreement, attached hereto in Attachment I, and incorporated herein by reference. County executed a HIPAA BAA with DHCS, which allows for MCP to share PHI with County under this MOU per CWDA and DSS.

b. PERSONALLY IDENTIFIABLE INFORMATION ("PII")

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

ii. MCP 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, 42 Code of Federal Regulations (CFR) section 431.300 et.seq, and 45 CFR 205.50 et.seq, 22 Cal. Code Regs. § 51009 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 COUNTY. MCP shall not duplicate, disseminate or disclose PII except as allowed in this MOU.

iii. MCP agrees to the PII Privacy and Security Standards attached as Attachment II.

c. **Use of Data and Data Exchange.** MCP must, and County is encouraged to, share the minimum necessary data and information to facilitate referrals and coordinate care under this MOU. The Parties must have policies and procedures for supporting the timely and frequent exchange of Member information and data, which may include behavioral health and physical health data; for ensuring the confidentiality of exchanged information and data; and, if necessary, for obtaining Member consent. The minimum necessary information and data elements to be shared as agreed upon by the Parties are set forth in Exhibit C of this MOU. The Parties must annually review and, if appropriate,

update Exhibit C of this MOU to facilitate sharing of information and data. The Parties are not required to obtain specific signed releases of information to exchange Member data for the purpose of sending and receiving referrals.

a. Any necessary changes to the data exchanged may be made jointly by the Parties without a formal amendment to this Agreement, unless such changes materially impact the scope or objectives of the Agreement. The determination of whether a change materially impacts the scope or objectives of the Agreement shall be made jointly by the Parties, in good faith, and with due consideration to the original intent and purpose of the Agreement. Any agreement between the Parties related to the necessary changes to the data exchanged shall be confirmed via email by both Parties.

i. MCP must coordinate with County to receive population data regarding IHSS-PA for Members to enable MCP to have more accurate and precise measurements of health risks and disparities within MCP's Member population, as required by the CalAIM Population Health Management Policy Guide.[2]

ii. MCP must, and County is encouraged to, share information necessary to facilitate referrals as described in Section 7 of this MOU and provide ongoing care coordination as described in Section 8 of this MOU. The data elements to be shared must be agreed upon jointly by the Parties, reviewed annually, and set forth in Exhibit C of this MOU.

iii. MCP must share information with County that is necessary for the IHSS-PA Liaison to identify which Members are also receiving ECM and/or Community Supports, to assist Members with accessing all available services.

If Member authorization is required, the Parties must agree to a standard consent form to obtain Member authorization to share and use information for the purposes of treatment, payment, and care coordination protected under 42 Code of Federal Regulations Part 2.

b. **Interoperability.** MCP must make available to Members their electronic health information held by MCP pursuant to 42 Code of Federal Regulations Section 438.10 and in accordance with APL 22-026 or any subsequent version of the APL. MCP must make available an application programming interface ("API") that makes complete and accurate Network Provider directory information available through a public-facing digital endpoint on MCP's website pursuant to 42 Code of Federal Regulations Sections 438.242(b) and 438.10(h).

12. Dispute Resolution.

a. The Parties must agree to dispute resolution procedures such that in the event of any dispute or difference of opinion regarding the Party responsible for service coverage arising out of or relating to this MOU, the Parties must attempt, in good faith, to promptly resolve the dispute mutually between themselves. MCP must, and IHSS-PA should, document the agreed-upon dispute resolution procedures in policies and procedures. Pending resolution of any such dispute, the Parties must continue without delay to carry out all their responsibilities under this MOU, including providing Members with access to services under this MOU, unless this MOU is terminated. If the dispute cannot be resolved

within 30 Working Days of initiating such dispute or such other period as may be mutually agreed to by the Parties in writing, either Party may pursue its available legal and equitable remedies under California law.

[2] CalAIM Population Health Management Policy Guide, available at https://www.dhcs.ca.gov/CalAIM/Documents/2023-PHM-Policy-Guide.pdf.

b. Disputes between MCP and County that cannot be resolved in a good faith attempt between the Parties must be forwarded by MCP to DHCS and may be reported by County to the California Department of Social Services. Until the dispute is resolved, the Parties may agree to an arrangement satisfactory to both Parties regarding how the services under dispute will be provided.

c. Nothing in this MOU or provision constitutes a waiver of any of the government claim filing requirements set forth in Title I, Division 3.6, of the California Government Code or otherwise set forth in local, State, or federal law.

13. Equal Treatment. Nothing in this MOU is intended to benefit or prioritize Members over persons served by IHSS-PA who are not Members. Pursuant to Title VI, 42 United States Code Section 2000d, et seq., County cannot provide any service, financial aid, or other benefit to an individual that is different, or is provided in a different manner, from that provided to others by IHSS-PA.

14. General.

a. **MOU Posting.** MCP must post this executed MOU on its website.

b. **Documentation Requirements.** MCP must retain all documents demonstrating compliance with this MOU for at least 10 years as required by the Medi Cal Managed Care Contract. If DHCS requests a review of any existing MOU, MCP must submit the requested MOU to DHCS within 10 Working Days of receipt of the request.

c. **Notice.** Any notice required or desired to be given pursuant to or in connection with this MOU must be given in writing, addressed to the noticed Party at the Notice Address set forth below the signature lines of this MOU. Notices must be (i) delivered in person to the Notice Address; (ii) delivered by messenger or overnight delivery service to the Notice Address; (iii) sent by regular United States mail, certified, return receipt requested, postage prepaid, to the Notice Address; or (iv) sent by email, with a copy sent by regular United States mail to the Notice Address. Notices given by in-person delivery, messenger, or overnight delivery service are deemed given upon actual delivery at the Notice Address. Notices given by email are deemed given the day following the day the email was sent. Notices given by regular United States mail, certified, return receipt requested, postage prepaid, are deemed given on the date of delivery indicated on the return receipt. The Parties may change their addresses for purposes of receiving notice hereunder by giving notice of such change to each other in the manner provided for herein.

d. **Delegation.** MCP may delegate its obligations under this MOU to a Fully Delegated Subcontractor or Partially Delegated Subcontractor as permitted under the Medi-Cal Managed Care Contract, provided that such Fully Delegated Subcontractor or Partially Delegated Subcontractor is made a Party to this MOU. Further, MCP may enter into Subcontractor Agreements or Downstream Subcontractor Agreements that relate directly or indirectly to the performance of MCP's obligations under this MOU. Other than in these circumstances, MCP cannot delegate the obligations and duties contained in this MOU.

e. **Annual Review.** MCP must conduct an annual review of this MOU to determine whether any modifications, amendments, updates, or renewals of responsibilities and obligations outlined within are required. Any recommendations for modifications, amendments, updates or renewals of responsibilities shall be brought forth to the county for consideration and discussion. MCP must provide DHCS evidence of the annual review of this MOU as well as copies of any MOU modified or renewed as a result.

f. **Amendment.** This MOU may only be amended or modified by the Parties through a writing executed by the Parties. This MOU shall be reviewed on an annual basis and as necessary upon issuance of new guidelines by the State, to determine the need to incorporate any changes pursuant to new policies issued by state agencies, MCP contract changes, or for other factors deemed appropriate by the MCP and IHSS agency. However, any amendments to current guidance or regulations applicable to Medi-Cal Managed Care Contract communicated through laws and statutes from the State of California or Federally shall be incorporated in this Agreement by reference and an amendment shall not be required.

g. **Governance.** This MOU is governed by and construed in accordance with the laws of the State of California.

h. **Independent Contractors.** No provision of this MOU is intended to create, nor is any provision deemed or construed to create, any relationship between County and MCP other than that of independent entities contracting with each other hereunder solely for the purpose of effecting the provisions of this MOU. Neither County nor MCP, nor any of their respective contractors, employees, agents, or representatives, is construed to be the contractor, employee, agent, or representative of the other.

i. **Counterpart Execution.** This MOU may be executed in counterparts, signed electronically and sent via PDF, each of which is deemed an original, but all of which, when taken together, constitute one and the same instrument.

j. **Superseding MOU.** This MOU constitutes the final and entire agreement between the Parties and supersedes any and all prior oral or written agreements, negotiations, or understandings between the Parties that conflict with the provisions set forth in this MOU. It is expressly understood and agreed that any prior written or oral agreement between the Parties pertaining to the subject matter herein is hereby terminated by mutual agreement of the Parties.

k. **Indemnification**. Both parties shall indemnify, and hold harmless, its officers, employees and agents from any liability whatsoever, including wrongful death, based or asserted upon any act or omission of, its employees, subcontractors and agents relating to or in any way connected with the accomplishment of the work or performance of service under this MOU. As part of the foregoing indemnity, both parties agree to protect and defend at its own expense, including attorneys' fees, its officers, agents and employees in any legal action based upon any such alleged acts or omissions. The terms of this Section shall survive the termination of this MOU.

l. **Insurance.** Without limiting or diminishing the MCP's obligation to indemnify or hold the COUNTY harmless, MCP shall procure and maintain or cause to be maintained, at its sole cost and expense, the following insurance coverage's during the term of this MOU. In respect to the insurance section only, the COUNTY herein refers to the County of Riverside, its Agencies, Districts, Special Districts, and Departments, their respective directors, officers, Board of Supervisors, employees, elected or appointed

officials, agents or representatives as Additional Insureds.

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

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

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

D. Cyber Liability Insurance, with limits not less than $2,000,000 per occurrence or claim, $2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by MCP in this MOU and shall include, but not limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations. If the MCP maintains broader coverage and/or higher limits than the minimums shown above, the COUNTY requires and shall be entitled to the broader coverage and/or higher limits maintained by the MCP. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to the COUNTY. Policy shall name the COUNTY as Additional Insureds.

General Insurance Provisions - All lines:

1) Any insurance carrier providing insurance coverage hereunder shall be admitted to the State of California and have an A M BEST rating of not less than A: VIII (A:8) unless such requirements are waived, in writing, by the County Risk Manager. If the County's Risk Manager waives a requirement for a particular insurer such waiver is only valid for that specific insurer and only for one policy term.

2) The MCP must declare its insurance self-insured retention for each coverage required herein. If any such self-insured retention exceed $500,000 per occurrence each

such retention shall have the prior written consent of the County Risk Manager before the commencement of operations under this MOU. Upon notification of self-insured retention unacceptable to the COUNTY, and at the election of the County's Risk Manager, MCP's carriers shall either; 1) reduce or eliminate such self-insured retention as respects this MOU with the COUNTY, or 2) procure a bond which guarantees payment of losses and related investigations, claims administration, and defense costs and expenses.

3) MCP shall cause MCP insurance carrier(s) to furnish the County of Riverside with either 1) a properly executed original Certificate(s) of Insurance and certified original copies of Endorsements effecting coverage as required herein, and 2) if requested to do so orally or in writing by the County Risk Manager, provide original Certified copies of policies including all Endorsements and all attachments thereto, showing such insurance is in full force and effect. Further, said Certificate(s) and policies of insurance shall contain the covenant of the insurance carrier(s) that a minimum of thirty (30) days written notice shall be given to the County of Riverside prior to any material modification, cancellation, expiration or reduction in coverage of such insurance. If MCP insurance carrier(s) policies does not meet the minimum notice requirement found herein, MCP shall cause MCP's insurance carrier(s) to furnish a 30 day Notice of Cancellation Endorsement.

4) In the event of a material modification, cancellation, expiration, or reduction in coverage, this MOU shall terminate forthwith, unless the County of Riverside receives, prior to such effective date, another properly executed original Certificate of Insurance and original copies of endorsements or certified original policies, including all endorsements and attachments thereto evidencing coverage's set forth herein and the insurance required herein is in full force and effect. MCP shall not commence operations until the COUNTY has been furnished original Certificate (s) of Insurance and certified original copies of endorsements and if requested, certified original policies of insurance including all endorsements and any and all other attachments as required in this Section. An individual authorized by the insurance carrier to do so on its behalf shall sign the original endorsements for each policy and the Certificate of Insurance.

5) It is understood and agreed to by the parties hereto that the MCP's insurance shall be construed as primary insurance, and the COUNTY'S insurance and/or deductibles and/or self-insured retentions or self-insured programs shall not be construed as contributory.

6) If, during the term of this MOU or any extension thereof, there is a material change in the scope of services; or, there is a material change in the equipment to be used in the performance of the scope of work; or, the term of this MOU, including any extensions thereof, exceeds five (5) years; the COUNTY reserves the right to adjust the types of insurance and the monetary limits of liability required under this MOU, if in the County Risk Management's reasonable judgment, the amount or type of insurance carried by the MCP has become inadequate.

7) MCP shall pass down the insurance obligations contained herein to all tiers of subcontractors working under this MOU.

8) The insurance requirements contained in this MOU may be met with a program(s) of self-insurance acceptable to the COUNTY.

9) MCP agrees to notify COUNTY of any claim by a third party or any incident or event that may give rise to a claim arising from the performance of this MOU.

m. **Compliance with Law.** The parties shall observe and comply with all

applicable local, state and federal laws, ordinances, rules and regulations now in effect or hereafter enacted, each of which is hereby made a part hereof and incorporated herein by reference.
The Parties represent that they have authority to enter into this MOU on behalf of their respective entities and have executed this MOU as of the Effective Date.

MCP

Signature:

Abbie Totten
Plan President
Molina Healthcare of California
Notice Address:
200 Oceangate
Long Beach, CA 90802

County of Riverside
Department of Public Social Services

Signature: David Dai

David Dai 05/06/2025
Executive Director

Notice Address:
County of Riverside
Department of Public Social Services
12125 Day Street,
Moreno Valley CA 92557

Approved as to Form
Minh C. Tran
County Counsel

By: Eric Stopher

Eric Stopher
Deputy County Counsel IV

05/06/2025
Date

Exhibits A and B

County IHSS-PA Liaison	Address	Telephone	e-mail
Vanessa Johnson, Regional Manager	12125 Day Street Moreno Valley, CA 92557	951-358-4868	dpss_asd_contract_support@rivco.org
David Dai, Executive Director	12125 Day Street Moreno Valley CA 92557	951-413-5495	dpss_asd_contract_support@rivco.org

MCP IHSS-PA Liaison	Address	Telephone	e-mail
Director, Healthcare Services,	200 Oceangate Long Beach, CA 90802	562-485-4966	blanca.martinez@molinahealthcare.com

Exhibit C

Data Elements

The Parties agree to share data elements such as:

a. Member demographic information;
b. Service referral receipt, information regarding client services offered/rendered, and outcome/closed loop information;
c. Known changes in condition that may adversely impact the Member's health and/or welfare and that are relevant to the services.

Attachment I

HIPAA Business Associate Agreement
Addendum to Contract
Between the County of Riverside and Molina Healthcare of California, Inc.

This HIPAA Business Associate Agreement (the "Addendum") supplements, and is made part of (the DPSS-0005261 "Underlying Agreement") between the County of Riverside ("County") and Molina Healthcare of California, Inc. ("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. <u>Scope of Use and Disclosure by Contractor of County's PHI and/or ePHI.</u>

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. <u>Prohibited Uses and Disclosures.</u>

A. Contractor may neither use, disclose, nor access PHI and/or ePHI in a manner not authorized by the Underlying Agreement or this Addendum without patient authorization or de-identification of the PHI and/or ePHI and as authorized in writing from County.

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

C. Contractor agrees not to make any disclosure of PHI and/or ePHI that County would be prohibited from making.

D. Contractor shall not use or disclose PHI for any purpose prohibited by the Privacy Rule, Security Rule, HIPAA and/or HITECH, including, but not limited to 42 USC §17935 and §17936. Contractor agrees:

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

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

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

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

4. Obligations of County.

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

B. County agrees to make its best efforts to promptly notify Contractor in writing of any changes in, or revocation of, permission by any individual to use or disclose PHI and/or ePHI, if such changes or revocation may affect Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.

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

D. County agrees not to request Contractor to use or disclose PHI and/or ePHI in any manner that would not be permissible under HITECH, HIPAA, the Privacy Rule, and/or Security Rule.

E. County agrees to obtain any authorizations necessary for the use or disclosure of PHI and/or ePHI, so that Contractor can perform its obligations under this Addendum and/or Underlying Agreement.

5. Obligations of Contractor. In connection with the use or disclosure of PHI and/or ePHI, Contractor agrees to:

A. Use or disclose PHI only if such use or disclosure complies with each applicable requirement 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 extent Contractor is to carry out County's obligations under the Privacy Rule.

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

6. **Access to PHI, Amendment and Disclosure Accounting.** Contractor agrees to:

A. **Access to PHI, including ePHI.** Provide access to PHI, including ePHI if maintained electronically, in a designated record set to County or an individual as directed by County, within five (5) days of request from County, to satisfy the requirements of 45 CFR §164.524.

B. **Amendment of PHI.** Make PHI available for amendment and incorporate amendments to PHI in a designated record set County directs or agrees to at the request of an individual, within fifteen (15) days of receiving a written request from County, in accordance with 45 CFR §164.526.

C. **Accounting of disclosures of PHI and electronic health record.** Assist County to fulfill its obligations to provide accounting of disclosures of PHI under 45 CFR §164.528 and, where applicable, electronic health records under 42 USC §17935(c) if Contractor uses or maintains electronic health records. Contractor shall:

(1) Document such disclosures of PHI and/or electronic health records, and information related to such disclosures, as would be required for County to respond to a request by an individual for an accounting of disclosures of PHI and/or electronic health record in accordance with 45 CFR §164.528.

(2) Within fifteen (15) days of receiving a written request from County, provide to County or any individual as directed by County information collected in accordance with this section to permit County to respond to a request by an individual for an accounting of disclosures of PHI and/or electronic health record.

(3) Make available for County information required by this Section 6.C for six (6) years preceding the individual's request for accounting of disclosures of PHI, and for three (3) years preceding the individual's request for accounting of disclosures of electronic health record.

7. **Security of ePHI.** In the event County discloses ePHI to Contractor or Contractor needs to create, receive, maintain, transmit or have access to County ePHI, in accordance with 42 USC §17931 and 45 CFR §164.314(a)(2)(i), and §164.306, Contractor shall:

A. Comply with the applicable requirements of the Security Rule, and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that Contractor creates, receives, maintains, or transmits on behalf of County in accordance with 45 CFR §164.308, §164.310, and §164.312;

B. Comply with each of the requirements of 45 CFR §164.316 relating to the implementation of policies, procedures and documentation requirements with respect to ePHI;

C. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;

D. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the Privacy Rule;

E. Ensure compliance with the Security Rule by Contractor's workforce;

F. In accordance with 45 CFR §164.308(b)(2), require that any subcontractors that create, receive, maintain, transmit, or access ePHI on behalf of Contractor agree through contract to the same restrictions and requirements contained in this Addendum and comply with the applicable requirements of the Security Rule;

G. Report to County any security incident of which Contractor becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410; and,

H. Comply with any additional security requirements that are applicable to covered entities in Title 42 (Public Health and Welfare) of the United States Code, as may be amended from time to time, including but not limited to HITECH.

8. **Breach of Unsecured PHI.** In the case of breach of unsecured PHI, Contractor shall comply with the applicable provisions of 42 USC §17932 and 45 CFR Part 164, Subpart D, including but not limited to 45 CFR §164.410.

   A. **Discovery and notification.** Following the discovery of a breach of unsecured PHI, Contractor shall notify County in writing of such breach without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, except as provided in 45 CFR §164.412.

      (1) **Breaches treated as discovered.** A breach is treated as discovered by Contractor as of the first day on which such breach is known to Contractor or, by exercising reasonable diligence, would have been known to Contractor, which includes any person, other than the person committing the breach, who is an employee, officer, or other agent of Contractor (determined in accordance with the federal common law of agency).

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

         (a) The identification of each individual whose unsecured PHI has been, or is reasonably believed by Contractor to have been accessed, acquired, used or disclosed during the breach;

         (b) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

         (c) A description of the types of unsecured PHI involved in the breach, such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved;

         (d) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

         (e) A brief description of what Contractor is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,

         (f) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.

   B. **Cooperation.** With respect to any breach of unsecured PHI reported by Contractor, Contractor shall cooperate with County and shall provide County with any information requested by County to enable County to fulfill in a timely manner its own reporting and notification obligations, including but not limited to providing notice to individuals, prominent media outlets and the Secretary in accordance with 42 USC §17932 and 45 CFR §164.404, §164.406 and §164.408.

   C. **Breach log.** To the extent breach of unsecured PHI involves less than 500 individuals, Contractor shall maintain a log or other documentation of such breaches and provide such log or other documentation on an annual basis to County not later than fifteen (15) days after the end of each calendar year for submission to the Secretary.

D. **Delay of notification authorized by law enforcement.** If Contractor delays notification of breach of unsecured PHI pursuant to a law enforcement official's statement that required notification, notice or posting would impede a criminal investigation or cause damage to national security, Contractor shall maintain documentation sufficient to demonstrate its compliance with the requirements of 45 CFR §164.412.

E. **Payment of costs.** With respect to any breach of unsecured PHI caused solely by the Contractor's failure to comply with one or more of its obligations under this Addendum and/or the provisions of HITECH, HIPAA, the Privacy Rule or the Security Rule, Contractor agrees to pay any and all costs associated with providing all legally required notifications to individuals, media outlets, and the Secretary. This provision shall not be construed to limit or diminish Contractor's obligations to indemnify, defend and hold harmless County under Section 9 of this Addendum.

F. **Documentation.** Pursuant to 45 CFR §164.414(b), in the event Contractor's use or disclosure of PHI and/or ePHI violates the Privacy Rule, Contractor shall maintain documentation sufficient to demonstrate that all notifications were made by Contractor as required by 45 CFR Part 164, Subpart D, or that such use or disclosure did not constitute a breach, including Contractor's completed risk assessment and investigation documentation.

G. **Additional State Reporting Requirements.** The parties agree that this Section 8.G applies only if and/or when County, in its capacity as a licensed clinic, health facility, home health agency, or hospice, is required to report unlawful or unauthorized access, use, or disclosure of medical information under the more stringent requirements of California Health & Safety Code §1280.15. For purposes of this Section 8.G, "unauthorized" has the meaning given such term in California Health & Safety Code §1280.15(j)(2).

(1) Contractor agrees to assist County to fulfill its reporting obligations to affected patients and to the California Department of Public Health ("CDPH") in a timely manner under the California Health & Safety Code §1280.15.

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

9. <u>Hold Harmless/Indemnification.</u>

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. <u>General Provisions.</u>

A. **Retention Period.** Whenever Contractor is required to document or maintain documentation pursuant to the terms of this Addendum, Contractor shall retain such documentation for 6 years from the date of its creation or as otherwise prescribed by law, whichever is later.

B. **Amendment.** The parties agree to take such action as is necessary to amend this Addendum from time to time as is necessary for County to comply with HITECH, the Privacy Rule, Security Rule, and HIPAA generally.

C. **Survival.** The obligations of Contractor under Sections 3, 5, 6, 7, 8, 9, 11.B and 12.A of this Addendum shall survive the termination or expiration of this Addendum.

D. **Regulatory and Statutory References.** A reference in this Addendum to a section in HITECH, HIPAA, the Privacy Rule and/or Security Rule means the section(s) as in effect or as amended.

E. **Conflicts.** The provisions of this Addendum shall prevail over any provisions in the Underlying Agreement that conflict or appear inconsistent with any provision in this Addendum.

F. **Interpretation of Addendum.**

(1) This Addendum shall be construed to be part of the Underlying Agreement as one document. The purpose is to supplement the Underlying Agreement to include the requirements of the Privacy Rule, Security Rule, HIPAA and HITECH.

(2) Any ambiguity between this Addendum and the Underlying Agreement shall be resolved to permit County to comply with the Privacy Rule, Security Rule, HIPAA and HITECH generally.

G. **Notices to County.** All notifications required to be given by Contractor to County pursuant to the terms of this Addendum shall be made in writing and delivered to the County both by fax and to both of the addresses listed below by either registered or certified mail return receipt requested or guaranteed overnight mail with tracing capability, or at such other address as County may hereafter designate. All notices to County provided by Contractor pursuant to this Section shall be deemed given or made when received by County.

County HIPAA Privacy Officer: HIPAA Privacy Manager

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

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

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

County Departmental Officer: _____

County Departmental Officer Title: _____

County Department Address: _____

County Department Fax Number: _____

ATTACHMENT II
PII Privacy and Security Standards

I. PHYSICAL SECURITY

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

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

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

C. Issue identification badges to CONTRACTOR staff.

D. Require CONTRACTOR staff to wear these badges where PII is used, disclosed, or stored.

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

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

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

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

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

II. TECHNICAL SECURITY CONTROLS

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

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

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

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

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

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

G. User IDs and Password Controls.
   1. All users must be issued a unique username 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
Riverside County Department of Public Social Services
Business Continuity/Assurance and Review Services
731 Palmyrita Ave.
Riverside, CA 92507
privacyincident@rivco.org