MEMORANDUM OF UNDERSTANDING

Between

Health Net
Molina Healthcare of California

And

Los Angeles County
Department of Children and Family Services

Memorandum of Understanding

This Memorandum of Understanding ("MOU") is entered into by Health Net, Molina Healthcare of California and Los Angeles County Department of Children and Family Services ("County"), effective as of upon the last date of signature date indicated on the signature page ("Effective Date").

WHEREAS, Managed Care Plan (MCP) is required under the Medi-Cal Managed Care Contract Exhibit A, Attachment III, which can be accessed here, to enter into this MOU, a binding and enforceable contractual agreement, to ensure that Medi-Cal Members enrolled, or eligible to enroll, in MCP and who are County Child Welfare involved and/or receive foster care services ("Members") are able to access and/or receive services in a coordinated manner from MCP and County; and

WHEREAS, Health Net contracts with Molina Healthcare of California to provide and arrange for network services and otherwise delegates part of its responsibilities related to effectuating this MOU to Molina;

WHEREAS, MCP, Health Net, Molina Healthcare of California, and County will be referred herein as a "Party" and collectively as "Parties" to this MOU;

WHEREAS, the Parties desire to ensure that Members receive MCP and County services set forth in this MOU in a coordinated, non-duplicative manner and to provide a process to continuously evaluate the quality of the care coordination provided.

NOW, THEREFORE, 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 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. **County Child Welfare Services:** means the services provided by the State's program for child protection services and interventions, including foster care, that are administered by County and monitored by the California Department of Social Services ("CDSS"), Children and Family Services Division.

    b. **MCP/Plan Responsible Person:** means the person designated by MCP/Plan to oversee the MCP/Plan coordination and communication with County and ensure MCP/Plan's compliance with this MOU as described in Section 4 of this MOU.

    c. **MCP/Plan-County Liaison:** means MCP/Plan's designated point of contact responsible for acting as the liaison between MCP/Plan and County as described in Section 4 of this MOU. The MCP/Plan-County 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's compliance officer as appropriate.

d. **MCP Child Welfare Liaison:** means the MCP/Plan's designated individual(s) assigned to ensure the needs of children and youth involved with child welfare are met as outlined in the Medi-Cal Managed Care Contract, DHCS Plan Letters ("APL"s, or other similar instructions).

e. **County 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. **County Liaison:** means County's designated point of contact responsible for acting as the liaison between County and MCP as described in Section 5 of this MOU. The County Liaison should 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 County Responsible Person as appropriate.

2. **Term and Termination**

a. This MOU is in effect as of last date of signature indicated on the signature page, also referred to as full execution date ("Effective Date") and continues for a period of 5 years with option to extend for additional 5 years ("Renewal Term"), unless terminated subject to the provision below or as amended in accordance with Section 14.f of this MOU.

b. At least 180 calendar days prior to the expiration of the Initial Term of this MOU, the Parties agree to meet and review the existing MOU terms and conditions, as may be amended, to determine whether to extend the MOU for an additional 5 years to create a Renewal Term, under the same terms and conditions with no further action by both Parties; or for Parties to enter into a new/replacement MOU.

c. The Initial Term and any applicable Renewal Term are collectively referenced herein as "Term", unless terminated subject to the provision below.

d. Notwithstanding the above, either Party may terminate this MOU with or without cause upon 30 calendar day's written notice to the other Party.

3. **Services Covered by This MOU.** This MOU governs the coordination between County and MCP for the delivery of care and services for Members who are receiving County Child Welfare Services.

4. **MCP/Plan Obligations**

a. **Provision of Covered Services:** MCP/Plan are responsible for authorizing Medically Necessary Covered Services, and for coordinating care for Members provided by MCP/Plan's Network Providers and other providers of carve-out programs, services, and benefits. MCP/Plan must ensure Members, and/or their caregivers or legal guardian(s), are provided with information regarding Covered Services for which they are eligible, including Medi-Cal for Kids and Teens (the Early and Periodic Screening, Diagnostic and Treatment benefit) services and other MCP/Plan covered services when indicated based on screening findings.

   i. MCP/Plan must provide and cover, or arrange for, as appropriate, all Medically Necessary Medi-Cal for Kids and Teens services, including Behavioral Health Treatment services.

   ii. For Members currently receiving Specialty Mental Health Services ("SMHS") or enrolled in an existing care management program, such as California Wraparound, Full Service Partnership, or Health Care Program for Children in Foster Care ("HCPCFC"), if the Mental Health Plan ("MHP") for SMHS, a SMHS provider contracted to the MHP/Plan, or the care management program has contracted with MCP/Plan to be an Enhanced Care Management ("ECM") Provider, MCP/Plan must assign the Member to the MHP/Plan, SMHS provider contracted to the MHP/Plan, or existing care management program as the ECM Provider unless the Member (or parent, legal guardian, or caretaker) requests otherwise.[1]

   iii. If a Member is enrolled in more than one existing care management program and those programs are each contracted ECM Providers, MCP/Plan must assign the Member to the MHP or existing care management program that the Member identifies as the Member's preferred ECM Provider or, if necessary, another ECM Provider that has capacity to accept the Member. However, if County is also an ECM Provider pursuant to a separate agreement between MCP/Plan and County for ECM services, this MOU does not govern County's provision of ECM services.

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

   i. Meet at least quarterly with the County Responsible Person and appropriate County program executives, as required by Section 9 of this MOU;

   ii. Report on MCP/Plan's compliance with the MOU to MCP/Plan's compliance officer no less frequently than quarterly. The compliance officer is responsible for MOU compliance oversight reports as part of

each organization's compliance program and must address any compliance deficiencies in accordance with respective compliance program policies;

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

iv. Ensure the appropriate level of MCP/Plan leadership (e.g., 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/Plan's employees responsible for carrying out activities under this MOU, and as applicable for Downstream Subcontractors, and Network Providers; and

vi. Serve, or designate a person at MCP/Plan to serve, as the MCP/Plan-County Liaison, the point of contact and liaison between MCP/Plan and County to coordinate care for children and youth receiving County Child Welfare Services. The MCP-County Liaison is listed in Exhibit A of this MOU. As appropriate, the MCP/Plan-County Liaison must also serve as a family advocate. MCP/Plan must notify County of any changes to the MCP/Plan- County 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.

c. **Child Welfare Liaison:** MCP/Plan must designate an individual(s) to serve as the MCP Child Welfare Liaison. To ensure the needs of children and youth involved with child welfare are met. In accordance with DHCS-issued standards and expectations for this role as set forth in the Medi-Cal Managed Care Contract, DHCS APLs or other similar instructions. The MCP-County Liaison and the MCP Child Welfare Liaison roles may be assigned to the same designated individual.

d. **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:** County is responsible for delivering and coordinating County Child Welfare Services, which may include coordination with an ECM Provider to ensure timely and appropriate access to Member benefits and services.

i. County Foster Care Public Health Nurses ("PHNs"), County- assigned probation officers, Community Health Workers, HCPCFC PHNs, child welfare case workers, and other county staff and/or secondary case managers, as applicable, should assist Members in accessing ECM, and, as appropriate, refer youth and children involved in child welfare to MCP for ECM.

b. **Oversight Responsibility:** The designated County Responsible Person, listed in Exhibit B of this MOU, is responsible for overseeing compliance with this MOU. The County Responsible Person serves, or may designate a person to serve, as the designated County Liaison, the point of contact and liaison with MCP/Plan. The County Liaison is listed in Exhibit B of this MOU. County may designate one or more liaisons by program or service line. County must notify MCP/Plan of changes to the County Liaison as soon as reasonably practical but no later than the date of change.

c. **Care Coordination:** County will implement mechanisms to identify barriers to care coordination for discussion with the MCP.

i. County will ensure training and education regarding provisions are provided to County's employees who carry out responsibilities under this MOU, as applicable.

ii. County will ensure Members, and/or their caregivers or legal guardian(s), are provided with information regarding Covered Services, including Medi-Cal for Kids and Teens services, for which they are eligible. County must refer Members to MCP for Medi-Cal for Kids and Teens services and other MCP Covered Services when indicated based on screening findings. If the child or youth indicates a need for mental health or substance use services, Member may be served by MCP and/or County's MHP in accordance with Section 8(d) of this MOU.

6. **Training and Education**

a. To ensure compliance with this MOU, MCP/Plan must provide training and orientation for its employees who carry out MCP's responsibilities under this MOU and, as applicable, for MCP/Plan's Network Providers, Subcontractors, and Downstream Subcontractors who assist MCP with carrying out 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/Plan must provide this training prior to all such persons or entities performing responsibilities under this MOU and to all such persons

or entities at least annually thereafter. MCP/Plan must require its Subcontractors and Downstream Subcontractors to provide training on relevant MOU requirements and County services to their Network Providers.

b. In accordance with health education standards as required by the Medi-Cal Managed Care Contract, MCP/Plan must provide Members and Network Providers with educational materials related to accessing Covered Services, including for services provided by County. In addition, MCP/Plan must provide its Network Providers with training on Medi-Cal for Kids and Teens services, utilizing the newly developed DHCS Medi-Cal for Kids and Teens Outreach and Education Toolkit as required by APL 23-005 or any subsequent version of the APL.

c. MCP/Plan 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 non-business hours.

d. The Parties are encouraged to develop training and education resources covering the services provided or arranged for by the Parties. The Parties are encouraged to share their training and educational materials with each other to ensure the information in their respective training and education materials includes an accurate set of services provided or arranged for by each Party and is consistent with MCP and County policies and procedures, and with clinical practice standards.

e. The Parties are encouraged to develop and share outreach communication materials and develop initiatives to share resources about MCP and County with individuals who may be eligible for MCP's Covered Services and/or County services.

f. County must distribute MCP's current training and educational materials in a timely manner to support the County Liaison, County-assigned HCPCFC social workers, County behavioral health providers, HCPCPFC public health nurses, Community Health Workers, County Health Education Specialists, and social workers and child welfare case workers in assisting Members with accessing Covered Services. The materials must include information on MCP's Covered Services, including nonemergency medical transportation and non-medical transportation; Community Supports; and/or other care management programs and services for which Members may qualify, such as ECM or Complex Care Management ("CCM").

7. **Referral Process**

Effective July 1, 2025, or date set forth by DHCS, MCP must comply with DHCS Closed-Loop Referral Implementation Guidance. For all referrals made to ECM, Community Supports, and future CLR-applicable services, MCP must implement

procedures to track, support, and monitor referrals submitted by County through referral closure. MCP must also adhere to requirements for notifying the County of the authorization status, referral loop closure reason and closure date within timeframes outlined in the guidance to support County in their awareness of referral status and outcomes for Members referred to CLR services. The Parties will work together collaboratively to establish the means and methods for MCP notifications for CLRs. DHCS requires MCPs to use electronic methods to notify referring entities of a referral's status, not paper-based methods.

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 Parties must discuss and address individual care planning and coordination issues or barriers to care coordination efforts no less than quarterly.

      iii. MCP/Plan 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.

      iv. MCP/Plan and County must collaborate to ensure that Members receiving County Child Welfare Services continue to receive all Medically Necessary Covered Services, including, without limitation, dental, behavioral, and developmental services, when they move to a new location or they transition or age out of receiving County foster care services.

      v. MCP/Plan must have processes for ensuring the continuation of Basic Population Health Management[1] and care coordination of all Medically Necessary Covered Services to be provided or arranged for by MCP/Plan for Members receiving County Child Welfare Services, with special attention to Members transitioning out of receiving foster care services and Members changing foster care placements.

      vi. MMCP/Plan's policies and procedures must include processes for

---

[1] CalAIM Population Health Management Policy Guide, available at: https://www.dhcs.ca.gov/CalAIM/Documents/2023-PHM-Policy-Guide-May-Update- 0509023.pdf.

[3] Basic Population Health Management is defined as described in the CalAIM Population Health Management Policy Guide, available at: https://www.dhcs.ca.gov/CalAIM/Documents/2023- PHM-Policy-Guide-May-Update-0509023.pdf.

coordinating with County to ensure enrolled Members (children, transition-aged foster youth, parents and caregivers) receive ECM, CCM, behavioral health and/or Community Supports and/or other case management services for which they may qualify and can help address social determinants of health.

vii. MCP/Plan must ensure Members' Medical Records are readily accessible and up to date for Members transitioning or aging out of receiving County foster care services.

viii. The Parties are encouraged to coordinate to identify Members not receiving periodic preventive services in accordance with the American Academy of Pediatrics ("AAP") Bright Futures Periodicity Schedule using a data-informed methodology and develop a plan to help providers reach out to assigned Members who are not receiving periodic preventive services.

ix. The Parties will develop policies and procedures to describe protocols for coordinating with other county departments and MCPs when children move between counties.

b. **Coordination of Medi-Cal for Kids and Teens Services**[3]

i. Where MCP/Plan and County have overlapping responsibilities to coordinate services for Members under age 21, MCP must do the following:

1. Assess the Member's medical and/or behavioral needs, or follow the Member's physician's or licensed behavioral health professional's recommendations, for Medi-Cal for Kids and Teens Medically Necessary Covered Services

2. Determine what types of services (if any) are being provided by County, or other third-party programs or services;

3. Coordinate the provision of services with County to ensure that MCP and County are not providing or ensuring the provision of duplicative services and that the Member is receiving all Medically Necessary Medi-Cal for Kids and Teens services within 60 calendar days following the preventive screening or other visit identifying a need for treatment, whether or not the services are Covered Services under the Medi-Cal Managed Care Contract. All Medi-Cal for Kids and Teens services are Covered Services unless expressly excluded under the Medi-Cal Managed Care Contract;

4. Notify the appropriate primary case manager, HCPCFC

PHN, and/or social/case worker if the Member (or parent, legal guardian, or caregiver) when the Member refuses services or is unable to be reached to ensure County has information necessary to inform investigations, guide county placement decisions, and/or alert County staff to issues of safety or neglect; and

5. Notify the appropriate primary case manager, HCPCFC PHN, and/or HCPCFC social worker at the assumption of care to ensure that the appropriate person is aware of all services being provided to the Member.

c. **Care Coordination for Youth and Children in Foster Care and their families/caregivers who are also MCP members**

i. MCP/Plan must implement policies and procedures to track Members receiving County Child Welfare Services by maintaining an up-to-date database of Members who are involved with child welfare and/or foster care as identified by the CDSS in collaboration with MCP/Plan.

ii. The MCP/Plan-County Liaison must oversee coordination of care for Members receiving County Child Welfare Services by:

1. Ensuring that each Member is assessed for medical and behavioral health needs

2. Ensuring that each Member's needs as defined under Medi-Cal for Kids and Teens services have been met through the provision of a care plan and warm hand offs to appropriate Providers. If services are needed, the first encounter must occur without unnecessary delay and in accordance with clinical standards (e.g., AAP Bright Futures Periodicity Schedule, Advisory Committee on Immunization Practices vaccination schedule). This includes collaborating with Providers, foster caregivers, and HCPCFC PHN as necessary to ensure medical and dental exams are provided within 30 calendar days in accordance with the Child Welfare Services Manual Division 31.206.36;

3. Notifying group homes, Short Term Residential Therapeutic Programs, HCPCFC staff, HCPCFC social workers and/or case managers, and foster parents of Members regarding MCP and County services when a Member is placed outside MCP's Service Area, as applicable;

4. Offering transportation information and resources, as needed, to Members, such as how Members can access non-emergency medical transportation for Medi-Cal services, which

include, but are not limited to, appointments and medication, medical equipment, and supplies pickup;

5. Upon request by County or a Network Provider, facilitating scheduling of medical appointments and referrals for dental services for Members;

6. Informing Network Providers about the availability of benefits, including dental benefits, such as assisting Members with scheduling appointments, including behavioral health appointments, and arranging non-emergency medical transportation for Medi-Cal services; and

7. Upon request, providing information regarding the Member's Primary Care Physician ("PCP") or other Network Provider to County to assist with coordination of care.

8. County should, when requested by Members (or Members' parent(s) or legal guardian(s) and/or caregiver(s) of foster children), assist Members ages 0-21 years with scheduling appointments for medical services through their assigned PCP and/or alert MCP of barriers to Members' access to services.

d. **Care Coordination for Specialty Mental Health Services and Substance Use Disorder Services for Youth and Children, and Caregivers who are MCP members**

i. MCP and County must coordinate to ensure that Members receiving County Child Welfare Services are directly referred to County's MHP for an SMHS assessment pursuant to BHIN 21-073 if they, or an individual acting on their behalf, contacts the MCP access line or the MHP seeking help.

ii. MCP must ensure that Members are provided with all Medically Necessary Covered Services, as identified by the assessments and communicated to MCP, in a timely and coordinated manner and in accordance with DHCS APLs 22-005, 22-006, and 22-028 or other forthcoming instructions.

iii. The Parties must develop a process for coordinating care for Members receiving County Child Welfare Services who are eligible for or are concurrently receiving Non-Specialty Mental Health Services ("NSMHS") and SMHS consistent with the No Wrong Door for Mental Health Services Policy described in APL 22-005 and BHIN 22-011.

iv. MCP must adopt a "no wrong door" referral process for Members and work collaboratively to ensure that Members may access NSMHS and SMHS through multiple pathways and are not turned away based on

which pathway they rely on, including but not limited to adhering to all applicable No Wrong Door for Mental Health Services Policy requirements described in APL 22-005 and BHIN 22-011.

v. The Parties are encouraged to coordinate to help ensure that Members receiving County Child Welfare Services, including parents and caregivers if they are Medi-Cal MCP enrollees, receive care navigation support in securing a non-specialty mental health appointment within timely access standards.

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 activities, Quality Improvement outcomes, systemic and case-specific concerns, and communicating with others within their organizations about such activities. These meetings may be conducted virtually.

i. 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.

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

iii. MCP must report to DHCS updates from quarterly meetings in a manner and frequency specified by DHCS.

b. **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, Child and Family Team Meetings, and County engagements, to collaborate with County in equity strategy and wellness and prevention activities.

10. **Quality Improvement:** The Parties must develop Quality Improvement activities specifically for the oversight of the requirements of this MOU, including, without limitation, any applicable performance measures and Quality Improvement

initiatives, including those to prevent duplication of services, as well as reports that track referrals, Member engagement, and service utilization, and population health measures. MCP must document these Quality Improvement activities in policies and procedures.

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 applicable law, which may include the Health Insurance Portability and Accountability Act and its implementing regulations, as amended ("HIPAA"), 42 Code of Federal Regulations Part 2, and other State and federal privacy laws. For additional guidance related to sharing Members' data and information, the Parties may reference the CalAIM Data Sharing Authorization Guidance, and Exhibit E of this MOU.

    a. **Data and/or Information 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 sharing authorization documentation and Member demographic, contact, behavioral, and physical health information; CANS data; diagnoses; relevant physical assessments and screenings for adverse childhood experiences; medications prescribed; documentation of social or environmental needs identified; individual nursing service plan ("INSP")/Case Plan; and known changes in condition that may adversely impact the Member's health and/or welfare; and, if necessary, obtaining member consent. The minimum necessary information and data elements to be shared quarterly 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.

        i. MCP/Plan must implement processes and procedures to ensure the Medical Records of those Members receiving County Child Welfare Services are readily accessible to ensure prompt information exchange and linkages to services, and to assist with ensuring that this population's complex needs remain met once Members are no longer involved with County Child Welfare and/or foster care.

        ii. MCP/Plan must share the necessary information with County to ensure the County Liaison is made aware of Members who are enrolled in ECM and/or Community Supports and (i) are receiving County Child Welfare Services; (ii) have been involved with foster care

in the past 12 months; (iii) are eligible for and/or enrolled in the Adoption Assistance Program;[2] or (iv) have received Family Maintenance services[3] in the past 12 months, in order to improve collaboration between County and ECM to help ensure Members have access to all available services.

iii. MCP/Plan and County will collaborate to develop processes and implement strategies to ensure their systems share data, and work together to improve outcomes that require collaboration across systems, including process measures (such as appropriate cross-sector attendance at Child and Family Teams Meetings), utilization measures (such as timely and appropriate access to Medi-Cal for Kids and Teens services for each Member), and outcome measures (such as shorter intervals until placement stability, shorter time to reunification, social drivers of health disparity gap closure).

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

v. To the extent Parties deem it necessary and/or appropriate, they can reference a business associate agreement (BAA) to be integrated into the Agreement by a reference in this subsection to a BAA as Exhibit D.

b. **Interoperability:** MCP/Plan must make available to Members their electronic health information held by MCP/Plan 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/Plan must make available an application programming interface 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 within 30 working days of issuance of the written statement by

the disputing Party. MCP/Plan must, and County should, document the agreed-upon dispute resolution procedures in policies and procedures. Pending resolution of any such dispute, County and MCP/Plan must continue without delay to carry out all their responsibilities under this MOU, including providing Members with access to services under this MOU, unless the MOU is terminated, in accordance with Section 2 of this MOU. If the dispute cannot be resolved within 90 Days of initiating such dispute or such other time 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.

b. Disputes between MCP/Plan and County that cannot be resolved in a good faith attempt between the Parties must be forwarded by MCP/Plan to DHCS and may be reported by County to CDSS. 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, and/or federal law.

13. **Equal Treatment:** Nothing in this MOU is intended to benefit or prioritize Members over persons served by County 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 County.

14. **General**

a. **MOU Posting:** MCP/Plan must post this executed MOU on its respective website.

b. **Documentation Requirements:** MCP/Plan 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 ten 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, Plan may enter into Downstream Subcontractor Agreements that relate directly or indirectly to the performance of MCP/Plan's obligations under this MOU. Other than in these circumstances, MCP/Plan cannot delegate the obligations and duties contained in this MOU.

e. **Annual Review:** MCP/Plan 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. MCP/Plan 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. However, this MOU is deemed automatically amended or modified to incorporate any provisions amended or modified in the Medi-Cal Managed Care Contract, or as required by applicable law or any applicable guidance issued by a State or federal oversight entity.

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/Plan 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/Plan, 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.

(Remainder of this page intentionally left blank)

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.

HEALTH NET

Signature: Dorothy Seleski

Name: Dorothy Seleski

Title: Medi-Cal President

Date: 03/26/2026

Notice Address:
21281 Burbank Boulevard, Woodland Hills, CA 91367

MOLINA HEALTHCARE OF CALIFORNIA

Signature: Abbie Ann Totten

Name: Abbie Totten

Title: Plan President

Date: 04/23/2026

Notice Address:
200 Oceangate, Suite 100, Long Beach, CA 90802

LOS ANGELES COUNTY DEPARTMENT OF CHILDREN AND FAMILY SERVICES

Signature:

Name: Brandon T. Nichols

Title: Director

Date: 05/15/26

Notice Address:
510 S. Vermont Avenue, Los Angeles, CA 90020

Exhibits A and B

TO
MEMORANDUM OF UNDERSTANDING

RESPONSIBLE PERSON / LIAISON

PROGRAM	Los Angeles County, Department of Children and Family Services (DCFS)	HEALTH NET (MCP)	MOLINA HEALTHCARE OF CALIFORNIA (MCP)
Responsible Person	Medical Director	Program Manager, MOU Compliance	Manager of Pediatric Case Management
Liaison	Office of the Medical Director Administrator	Community Liaison	Case Management (Foster Care)

Exhibit C

Data Elements

County and MCP will work collaboratively within the first year of executing the MOU to develop protocols for sharing information in accordance with this MOU and state and federal privacy laws. Examples of the types of information that the parties may share for purposes of care coordination in accordance with state and federal privacy laws, include:

A. From the County to the MCP:

- List of providers delivering child welfare services
- Additional data required to facilitate referrals and coordinate care, such as:
    - Member demographic information
    - Member contact information
    - Behavioral and physical health information
    - CANS data

B. From the MCP to the County:

- Relevant individual health information, such as diagnoses, medications, and utilization, that is the minimum necessary for care coordination, subject to any applicable authorization requirements.
- Data reflecting utilization, access and outcome metrics for the Members receiving child welfare services that are to be tracked in the MCP's up-to-date database per Section 8(c)(i) of this MOU. Examples of metrics from Section 11(a) may include:
    - Member demographic information
    - Member contact information
    - Diagnoses
    - Referral status
    - Service utilization rates for non-specialty mental health services community supports, enhanced care management and community health worker services, emergency department and inpatient hospitalization data.
    - Population health measures

EXHIBIT D

INFORMATION SECURITY AND PRIVACY

REQUIREMENTS EXHIBIT

The County of Los Angeles ("County") is committed to safeguarding the Integrity of the County systems, Data, Information and protecting the privacy rights of the individuals that it serves. This Information Security and Privacy Requirements Exhibit ("Exhibit") sets forth the County and the Managed care plan's commitment and agreement to fulfill each of their obligations under applicable state or federal laws, rules, or regulations, as well as applicable industry standards concerning privacy, Data protections, Information Security, Confidentiality, Availability, and Integrity of such Information. The Information Security and privacy requirements and procedures in this Exhibit are to be established by the Managed care plan before the Effective Date of the MOU and maintained throughout the term of the MOU.

These requirements and procedures are a minimum standard and are in addition to the requirements of the underlying base agreement between the County and Managed care plan (the "MOU") and any other agreements between the parties. However, it is the Managed care plan's sole obligation to: (i) implement appropriate and reasonable measures to secure and protect its systems and all County Information against internal and external Threats and Risks; and (ii) continuously review and revise those measures to address ongoing Threats and Risks. Failure to comply with the minimum requirements and procedures set forth in this Exhibit will constitute a material, non-curable breach of MOU by the Managed care plan, entitling the County, in addition to the cumulative of all other remedies available to it at law, in equity, or under the MOU, to immediately terminate the MOU. To the extent there are conflicts between this Exhibit and the MOU, this Exhibit shall prevail unless stated otherwise.

1. DEFINITIONS

Unless otherwise defined in the MOU, the definitions herein contained are specific to the uses within this exhibit.

a. **Availability:** the condition of Information being accessible and usable upon demand by an authorized entity (Workforce Member or process).

b. **Confidentiality:** the condition that Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the Information.

c. **County Information:** all Data and Information belonging to the County.

d. **Data:** a subset of Information comprised of qualitative or quantitative values.

Incident: a suspected, attempted, successful, or imminent Threat of unauthorized electronic and/or physical access, use, disclosure, breach, modification, or destruction of information; interference with Information Technology operations; or significant violation of County policy.

f. **Information:** any communication or representation of knowledge or understanding such as facts, Data, or opinions in any medium or form, including electronic, textual, numerical, graphic, cartographic, narrative, or audiovisual.

g. **Information Security Policy:** high level statements of intention and direction of an organization used to create an organization's Information Security Program as formally expressed by its top management.

h. **Information Security Program:** formalized and implemented Information Security Policies, standards and procedures that are documented describing the program management safeguards and common controls in place or those planned for meeting the County's information security requirements.

i. **Information Technology:** any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of Data or Information.

j. **Integrity**: the condition whereby Data or Information has not been improperly modified or destroyed and authenticity of the Data or Information can be ensured.

k. **Mobile Device Management (MDM):** software that allows Information Technology administrators to control, secure, and enforce policies on smartphones, tablets, and other endpoints.

l. **Privacy Policy:** high level statements of intention and direction of an organization used to create an organization's Privacy Program as formally expressed by its top management.

m. **Privacy Program:** A formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the organization's privacy official and other staff, the strategic goals and objectives of the Privacy Program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

n. **Risk:** a measure of the extent to which the County is threatened by a potential circumstance or event, Risk is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

o. **Threat:** any circumstance or event with the potential to adversely impact County operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an Information System via unauthorized access, destruction, disclosure, modification of Information, and/or denial of service.

p. **Vulnerability:** a weakness in a system, application, network or process that is subject to exploitation or misuse.

q. **Workforce Member:** employees, volunteers, and other persons whose conduct, in the performance of work for Los Angeles County, is under the direct control of Los Angeles County, whether or not they are paid by Los Angeles County. This includes, but may not be limited to, full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to the County.

2. INFORMATION SECURITY AND PRIVACY PROGRAMS

a. **Information Security Program.** The Managed care plan shall maintain a company-wide Information Security Program designed to evaluate Risks to the Confidentiality, Availability, and Integrity of the County Information covered under this MOU.

Managed care plan's Information Security Program shall include the creation and maintenance of Information Security Policies, standards, and procedures. Information Security Policies, standards, and procedures will be communicated to all Managed care plan employees in a relevant, accessible, and understandable form and will be regularly reviewed and evaluated to ensure operational effectiveness, compliance with all applicable laws and regulations, and addresses new and emerging Threats and Risks.

The Managed care plan shall exercise the same degree of care in safeguarding and protecting County Information that the Managed care plan exercises with respect to its own Information and Data, but in no event less than a reasonable degree of care. The Managed care plan will implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the Confidentiality, Integrity, and Availability of County Information.

The Managed care plan's Information Security Program shall:

- Protect the Confidentiality, Integrity, and Availability of County Information in the Managed care plan's possession or control;
- Protect against any anticipated Threats or hazards to the Confidentiality, Integrity, and Availability of County Information;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of County Information;
- Protect against accidental loss or destruction of, or damage to, County Information; and
- Safeguard County Information in compliance with any applicable laws and regulations which apply to the Managed care plan.

b. **Privacy Program.** The Managed care plan shall establish and maintain a company-wide Privacy Program designed to incorporate Privacy Policies and practices in its business operations to

provide safeguards for Information, including County Information. The Managed care plan's Privacy Program shall include the development of, and ongoing reviews and updates to Privacy Policies, guidelines, procedures and appropriate workforce privacy training within its organization. These Privacy Policies, guidelines, procedures, and appropriate training will be provided to all Managed care plan employees, agents, and volunteers. The Managed care plan's Privacy Policies, guidelines, and procedures shall be continuously reviewed and updated for effectiveness and compliance with applicable laws and regulations, and to appropriately respond to new and emerging Threats and Risks. The Managed care plan's Privacy Program shall perform ongoing monitoring and audits of operations to identify and mitigate privacy Threats.

The Managed care plan shall exercise the same degree of care in safeguarding the privacy of County Information that the Managed care plan exercises with respect to its own Information, but in no event less than a reasonable degree of care. The Managed care plan will implement, maintain, and use appropriate privacy practices and protocols to preserve the Confidentiality of County Information.

The Managed care plan's Privacy Program shall include:

- A Privacy Program framework that identifies and ensures that the Managed care plan complies with all applicable laws and regulations;
- External Privacy Policies, and internal privacy policies, procedures and controls to support the privacy program;
- Protections against unauthorized or unlawful access, use, disclosure, alteration, or destruction of County Information;
- A training program that covers Privacy Policies, protocols and awareness;
- A response plan to address privacy Incidents and privacy breaches; and
- Ongoing privacy assessments and audits.

3. PROPERTY RIGHTS TO COUNTY INFORMATION

All County Information is deemed property of the County, and the County shall retain exclusive rights and ownership thereto. County Information shall not be used by the Managed care plan for any purpose other than as required under this MOU, nor shall such or any part of such be disclosed, sold, assigned, leased, or otherwise disposed of, to third parties by the Managed care plan, or commercially exploited or otherwise used by, or on behalf of, the Managed care plan, its officers, directors, employees, or agents. The Managed care plan may assert no lien on or right to withhold from the County, any County Information it receives from, receives addressed to, or stores on behalf of, the County. Notwithstanding the foregoing, the Managed care plan may aggregate, compile, and use County Information in order to improve, develop or enhance the System Software and/or other services offered, or to be offered, by the Managed care plan, provided that (i) no County Information in such aggregated or compiled pool is identifiable as

originating from, or can be traced back to the County, and (ii) such Data or Information cannot be associated or matched with the identity of an individual alone, or linkable to a specific individual. The Managed care plan specifically consents to the County's access to such County Information held, stored, or maintained on any and all devices Contactor owns, leases or possesses.

4. MANAGED CARE PLAN'S USE OF COUNTY INFORMATION

The Managed care plan may use County Information only as necessary to carry out its obligations under this MOU. The Managed care plan shall collect, maintain, or use County Information only for the purposes specified in the MOU and, in all cases, in compliance with all applicable local, state, and federal laws and regulations governing the collection, maintenance, transmission, dissemination, storage, use, and destruction of County Information, including, but not limited to, (i) any state and federal law governing the protection of personal Information, (ii) any state and federal security breach notification laws, and (iii) the rules, regulations and directives of the Federal Trade Commission, as amended from time to time.

5. SHARING COUNTY INFORMATION AND DATA

The Managed care plan shall not share, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, County Information to a third party for monetary or other valuable consideration.

6. CONFIDENTIALITY

a. **Confidentiality of County Information.** The Managed care plan agrees that all County Information is Confidential and proprietary to the County regardless of whether such Information was disclosed intentionally or unintentionally, or marked as "confidential".

b. **Disclosure of County Information.** The Managed care plan may disclose County Information only as necessary to carry out its obligations under this MOU, or as required by law, and is prohibited from using County Information for any other purpose without the prior express written approval of the County's MOU administrator in consultation with the County's Chief Information Security Officer and/or Chief Privacy Officer. If required by a court of competent jurisdiction or an administrative body to disclose County Information, the Managed care plan shall notify the County's MOU administrator immediately and prior to any such disclosure, to provide the County an opportunity to oppose or otherwise respond to such disclosure, unless prohibited by law from doing so.

c. **Disclosure Restrictions of Non-Public Information.** While performing work under the MOU, the Managed care plan may encounter County Non-public Information ("NPI") in the course of performing this MOU, including, but not limited to, licensed technology, drawings, schematics, manuals, sealed court records, and other materials described and/or identified as "Internal Use", "Confidential" or "Restricted"

as defined in Board of Supervisors Policy 6.104 – Information Classification Policy as NPI. The Managed care plan shall not disclose or publish any County NPI and material received or used in performance of this MOU. This obligation is perpetual.

d. **Individual Requests.** The Managed care plan shall acknowledge any request or instructions from the County regarding the exercise of any individual's privacy rights provided under applicable federal or state laws. The Managed care plan shall have in place appropriate policies and procedures to promptly respond to such requests and comply with any request or instructions from the County within seven (7) calendar days. If an individual makes a request directly to the Managed care plan involving County Information, the Managed care plan shall notify the County within five (5) calendar days and the County will coordinate an appropriate response, which may include instructing the Managed care plan to assist in fulfilling the request. Similarly, if the Managed care plan receives a privacy or security complaint from an individual regarding County Information, the Managed care plan shall notify the County as described in Section 14 SECURITY AND PRIVACY INCIDENTS, and the County will coordinate an appropriate response.

e. **Retention of County Information.** The Managed care plan shall not retain any County Information for any period longer than necessary for the Managed care plan to fulfill its obligations under the MOU and applicable law, whichever is longest.

7. MANAGED CARE PLAN EMPLOYEES

The Managed care plan shall perform background and security investigation procedures in the manner prescribed in this section unless the MOU prescribes procedures for conducting background and security investigations and those procedures are no less stringent than the procedures described in this section.

To the extent permitted by applicable law, the Managed care plan shall screen and conduct background investigations on all Managed care plan employees and Submanaged care plans as appropriate to their role, with access to County Information for potential security Risks. Such background investigations must be obtained through fingerprints submitted to the California Department of Justice to include State, local, and federal-level review and conducted in accordance with the law, may include criminal and financial history to the extent permitted under the law, and will be repeated on a regular basis. The fees associated with the background investigation shall be at the expense of the Managed care plan, regardless of whether the member of the Managed care plan's staff passes or fails the background investigation. The Managed care plan, in compliance with its legal obligations, shall conduct an individualized assessment of their employees, agents, and volunteers regarding the nature and gravity of a criminal offense or conduct; the time that has passed since a criminal offense or conduct and completion of the sentence; and the nature of the access to County Information to ensure that no individual accesses County Information whose past criminal conduct poses a risk or threat to County Information.

The Managed care plan shall require all employees, agents, and volunteers to abide by the requirements in this Exhibit, as set forth in the MOU, and sign an appropriate written Confidentiality/non-disclosure agreement with the Managed care plan.

The Managed care plan shall supply each of its employees with appropriate, annual training regarding Information Security procedures, Risks, and Threats. The Managed care plan agrees that training will cover, but may not be limited to the following topics:

a. **Secure Authentication:** The importance of utilizing secure authentication, including proper management of authentication credentials (login name and password) and multi-factor authentication.

b. **Social Engineering Attacks:** Identifying different forms of social engineering including, but not limited to, phishing, phone scams, and impersonation calls.

c. **Handling of County Information:** The proper identification, storage, transfer, archiving, and destruction of County Information.

d. **Causes of Unintentional Information Exposure:** Provide awareness of causes of unintentional exposure of Information such as lost mobile devices, emailing Information to inappropriate recipients, etc.

e. **Identifying and Reporting Incidents:** Awareness of the most common indicators of an Incident and how such indicators should be reported within the organization.

f. **Privacy:** The Managed care plan's Privacy Policies and procedures as described in Section 2b. Privacy Program.

The Managed care plan shall have an established set of procedures to ensure the Managed care plan's employees promptly report actual and/or suspected breaches of security.

8. SUBMANAGED CARE PLANS AND THIRD PARTIES

The County acknowledges that in the course of performing its services, the Managed care plan may desire or require the use of goods, services, and/or assistance of Submanaged care plans or other third parties or suppliers. The terms of this Exhibit shall also apply to all Submanaged care plans and third parties. The Managed care plan or third party shall be subject to the following terms and conditions: (i) each Submanaged care plan and third party must agree in writing to comply with and be bound by the applicable terms and conditions of this Exhibit, both for itself and to enable the Managed care plan to be and remain in compliance with its obligations hereunder, including those provisions relating to Confidentiality, Integrity, Availability, disclosures, security, and such other terms and conditions as may be reasonably necessary to effectuate the MOU including this Exhibit; and (ii) the Managed care plan shall be and remain fully liable for the acts and omissions of each Submanaged care plan and third party, and fully responsible for the due and proper performance of all Managed care plan obligations under this MOU.

The Managed care plan shall obtain advanced approval from the County's Chief Information Security Officer and/or Chief Privacy Officer prior to subMOUing services subject to this Exhibit.

9. STORAGE AND TRANSMISSION OF COUNTY INFORMATION

All County Information shall be rendered unusable, unreadable, or indecipherable to unauthorized individuals. Without limiting the generality of the foregoing, the Managed care plan will encrypt all workstations, portable devices (such as mobile, wearables, tablets,) and removable media (such as portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) that store County Information in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise approved by the County's Chief Information Security Officer.

The Managed care plan will encrypt County Information transmitted on networks outside of the Managed care plan's control with Transport Layer Security (TLS) or Internet Protocol Security **(**IPSec**)**, at a minimum cipher strength of 128 bit or an equivalent secure transmission protocol or method approved by County's Chief Information Security Officer.

In addition, the Managed care plan shall not store County Information in the cloud or in any other online storage provider without written authorization from the County's Chief Information Security Officer. All mobile devices storing County Information shall be managed by a Mobile Device Management system. Such system must provide provisions to enforce a password/passcode on enrolled mobile devices. All workstations/Personal Computers (including laptops, 2-in-1s, and tablets) will maintain the latest operating system security patches, and the latest virus definitions. Virus scans must be performed at least monthly. Request for less frequent scanning must be approved in writing by the County's Chief Information Security Officer.

10. RETURN OR DESTRUCTION OF COUNTY INFORMATION

The Managed care plan shall return or destroy County Information in the manner prescribed in this section unless the MOU prescribes procedures for returning or destroying County Information and those procedures are no less stringent than the procedures described in this section.

Return or Destruction. Upon County's written request, or upon expiration or termination of this MOU for any reason, Managed care plan shall (i) promptly return or destroy, at the County's option, all originals and copies of all documents and materials it has received containing County Information; or (ii) if return or destruction is not permissible under applicable law, continue to protect such Information in accordance with the terms of this MOU; and (iii) deliver or destroy, at the County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-readable form, prepared by the Managed care plan, prepared under its direction, or at its request, from the documents and materials referred to in Subsection (i) of this Section. For all documents or materials referred to in Subsections (i) and (ii) of this Section that the County requests be returned to the County, the Managed care plan shall provide a written attestation on

company letterhead certifying that all documents and materials have been delivered to the County. For documents or materials referred to in Subsections (i) and (ii) of this Section that the County requests be destroyed, the Managed care plan shall provide an attestation on company letterhead and certified documentation from a media destruction firm consistent with subdivision b of this Section. Upon termination or expiration of the MOU or at any time upon the County's request, the Managed care plan shall return all hardware, if any, provided by the County to the Managed care plan. The hardware should be physically sealed and returned via a bonded courier, or as otherwise directed by the County.

a. **Method of Destruction.** The Managed care plan shall destroy all originals and copies by (i) cross-cut shredding paper, film, or other hard copy media so that the Information cannot be read or otherwise reconstructed; and (ii) purging, or destroying electronic media containing County Information consistent with NIST Special Publication 800-88, "Guidelines for Media Sanitization" such that the County Information cannot be retrieved. The Managed care plan will provide an attestation on company letterhead and certified documentation from a media destruction firm, detailing the destruction method used and the County Information involved, the date of destruction, and the company or individual who performed the destruction. Such statement will be sent to the designated County MOU manager within ten (10) days of termination or expiration of the MOU or at any time upon the County's request. On termination or expiration of this MOU, the County will return or destroy all Managed care plan's Information marked as confidential (excluding items licensed to the County hereunder, or that provided to the County by the Managed care plan hereunder), at the County's option.

11. PHYSICAL AND ENVIRONMENTAL SECURITY

All Managed care plan facilities that process County Information will be located in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physically secure environment from unauthorized access, damage, and interference.

All Managed care plan facilities that process County Information will be maintained with physical and environmental controls (temperature and humidity) that meet or exceed hardware manufacturer's specifications.

12. OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY

The Managed care plan shall: (i) monitor and manage all of its Information processing facilities, including, without limitation, implementing operational procedures, change management, and Incident response procedures consistent with Section 14 SECURITY AND PRIVACY INCIDENTS; and (ii) deploy adequate anti-malware software and adequate back-up systems to ensure essential business Information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures are adequately documented and designed to protect Information and computer media from theft and unauthorized access.

The Managed care plan must have business continuity and disaster recovery plans. These plans must include a geographically separate back-up data center and a formal framework by which an unplanned event will be managed to minimize the loss of County Information and services. The formal framework includes a defined back-up policy and associated procedures, including documented policies and procedures designed to: (i) perform back-up of data to a remote back-up data center in a scheduled and timely manner; (ii) provide effective controls to safeguard backed-up data; (iii) securely transfer County Information to and from back- up location; (iv) fully restore applications and operating systems; and (v) demonstrate periodic testing of restoration from back-up location. If the Managed care plan makes backups to removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION), all such backups shall be encrypted in compliance with the encryption requirements noted above in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

13. ACCESS CONTROL

Subject to and without limiting the requirements under Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION, County Information (i) may only be made available and accessible to those parties explicitly authorized under the MOU or otherwise expressly approved by the County Project

Director or Project Manager in writing; and (ii) if transferred using removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be sent via a bonded courier and protected using encryption technology designated by the Managed care plan and approved by the County's Chief Information Security Officer in writing. The foregoing requirements shall apply to back-up media stored by the Managed care plan at off-site facilities.

The Managed care plan shall implement formal procedures to control access to County systems, services, and/or Information, including, but not limited to, user account management procedures and the following controls:

a. Network access to both internal and external networked services shall be controlled, including, but not limited to, the use of industry standard and properly configured firewalls;

b. Operating systems will be used to enforce access controls to computer resources including, but not limited to, multi-factor authentication, use of virtual private networks (VPN), authorization, and event logging;

c. The Managed care plan will conduct regular, no less often than semi-annually, user access reviews to ensure that unnecessary and/or unused access to County Information is removed in a timely manner;

d. Applications will include access control to limit user access to County Information and application system functions;

e. All systems will be monitored to detect deviation from access control policies and identify suspicious activity. The Managed care plan shall record, review and act upon all events in

accordance with Incident response policies set forth in Section 14 SECURITY AND PRIVACY INCIDENTS; and

f. In the event any hardware, storage media, or removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be disposed of or sent off-site for servicing, the Managed care plan shall ensure all County Information, has been eradicated from such hardware and/or media using industry best practices as discussed in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

14. SECURITY AND PRIVACY INCIDENTS

In the event of a Security or Privacy Incident, the Managed care plan shall:

a. Promptly notify the DCFS's Chief Information Security Officer, of any Incidents involving County Information, within twenty-four (24) hours of detection of the Incident. All notifications shall be submitted via encrypted email and telephone.

DCFS Information Security Officer:

Allen Ohanian (323) 567 9855

aohanian@dcfs.lacounty.gov; DCFSSecurity@dcfs.lacounty.gov

b. Include the following information in all notices:

i. The date and time of discovery of the Incident,

ii. The approximate date and time of the Incident,

iii. A description of the type of County Information involved in the reported Incident, and
iv. A summary of the relevant facts, including a description of measures being taken to respond to and remediate the Incident, and any planned corrective actions as they are identified.

v. The name and contact information for the organizations official representative(s), with relevant business and technical information relating to the incident.

c. Cooperate with the County to investigate the Incident and seek to identify the specific County Information involved in the Incident upon the County's written request, without charge, unless the Incident was caused by the acts or omissions of the County. As Information about the Incident is collected or otherwise becomes available to the Managed care plan, and unless prohibited by law, the Managed care plan shall provide Information regarding the nature and consequences of the

Incident that are reasonably requested by the County to allow the County to notify affected individuals, government agencies, and/or credit bureaus.

d. Immediately initiate the appropriate portions of their Business Continuity and/or Disaster Recovery plans in the event of an Incident causing an interference with Information Technology operations.

e. Assist and cooperate with forensic investigators, the County, law firms, and and/or law enforcement agencies at the direction of the County to help determine the nature, extent, and source of any Incident, and reasonably assist and cooperate with the County on any additional disclosures that the County is required to make as a result of the Incident.

f. Allow the County or its third-party designee at the County's election to perform audits and tests of the Managed care plan's environment that may include, but are not limited to, interviews of relevant employees, review of documentation, or technical inspection of systems, as they relate to the receipt, maintenance, use, retention, and authorized destruction of County Information.

Notwithstanding any other provisions in this MOU and Exhibit, The Managed care plan shall be (i) liable for all damages and fines, (ii) responsible for all corrective action, and (iii) responsible for all notifications arising from an Incident involving County Information caused by the Managed care plan's weaknesses, negligence, errors, or lack of Information Security or privacy controls or provisions.

15. NON-EXCLUSIVE EQUITABLE REMEDY

The Managed care plan acknowledges and agrees that due to the unique nature of County Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach may result in irreparable harm to the County, and therefore, that upon any such breach, the County will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies are available within law or equity. Any breach of Section 6 CONFIDENTIALITY shall constitute a material breach of this MOU and be grounds for immediate termination of this MOU in the exclusive discretion of the County.

16. AUDIT AND INSPECTION

a. **Self-Audits.** The Managed care plan shall periodically conduct audits, assessments, testing of the system of controls, and testing of Information Security and privacy procedures, including penetration testing, intrusion detection, and firewall configuration reviews. These periodic audits will be conducted by staff certified to perform the specific audit in question at Managed care plan's sole cost and expense through either (i) an internal independent audit function, (ii) a nationally recognized, external, independent auditor, or (iii) another independent auditor approved by the County.

The Managed care plan shall have a process for correcting control deficiencies that have been identified in the periodic audit, including follow up documentation providing evidence of such corrections. The Managed care plan shall provide the audit results and any corrective action documentation to the County promptly upon its completion at the County's request. With respect to any other report, certification, or audit or test results prepared or received by the Managed care plan that contains any County Information, the Managed care plan shall promptly provide the County with copies of the same upon the County's reasonable request, including identification of any failure or exception in the Managed care plan's Information systems, products, and services, and the corresponding steps taken by the Managed care plan to mitigate such failure or exception. Any reports and related materials provided to the County pursuant to this Section shall be provided at no additional charge to the County.

b. **County Requested Audits.** At its own expense, the County, or an independent third-party auditor commissioned by the County, shall have the right to audit the Managed care plan's infrastructure, security and privacy practices, Data center, services and/or systems storing or processing County Information via an onsite inspection at least once a year. Upon the County's request the Managed care plan shall complete a questionnaire regarding Managed care plan's Information Security and/or program. The County shall pay for the County requested audit unless the auditor finds that the Managed care plan has materially breached this Exhibit, in which case the Managed care plan shall bear all costs of the audit**;** and if the audit reveals material non- compliance with this Exhibit, the County may exercise its termination rights underneath the MOU.

   Such audit shall be conducted during the Managed care plan's normal business hours with reasonable advance notice, in a manner that does not materially disrupt or otherwise unreasonably and adversely affect the Managed care plan's normal business operations. The County's request for the audit will specify the scope and areas (e.g., Administrative, Physical, and Technical) that are subject to the audit and may include, but are not limited to physical controls inspection, process reviews, policy reviews, evidence of external and internal Vulnerability scans, penetration test results, evidence of code reviews, and evidence of system configuration and audit log reviews. It is understood that the results may be filtered to remove the specific Information of other Managed care plan customers such as IP address, server names, etc. The Managed care plan shall cooperate with the County in the development of the scope and methodology for the audit, and the timing and implementation of the audit. This right of access shall extend to any regulators with oversight of the County. The Managed care plan agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

   When not prohibited by regulation, the Managed care plan will provide to the County a summary of: (i) the results of any security audits, security reviews, or other relevant audits, conducted by the Managed care plan or a third party; and (ii) corrective actions or modifications, if any, the Managed care plan will implement in response to such audits.

17. CYBER LIABILITY INSURANCE

The Managed care plan shall secure and maintain cyber liability insurance coverage in the manner prescribed in this section unless the MOU prescribes cyber liability insurance coverage provisions and those provisions are no less stringent than those described in this section.

The Managed care plan shall secure and maintain cyber liability insurance coverage with limits of at least $5,000,000 per occurrence and in the aggregate during the term of the MOU, including coverage for: network security liability; privacy liability; privacy regulatory proceeding defense, response, expenses and fines; technology professional liability (errors and omissions); privacy breach expense reimbursement (liability arising from the loss or disclosure of County Information no matter how it occurs); system breach; denial or loss of service; introduction, implantation, or spread of malicious software code; unauthorized access to or use of computer systems; and Data/Information loss and business interruption; any other liability or risk that arises out of the MOU. The Managed care plan shall add the County as an additional insured to its cyber liability insurance policy and provide to the County certificates of insurance evidencing the foregoing upon the County's request. The procuring of the insurance described herein, or delivery of the certificates of insurance described herein, shall not be construed as a limitation upon the Managed care plan's liability or as full performance of its indemnification obligations hereunder. No exclusion/restriction for unencrypted portable devices/media may be on the policy.

18. PRIVACY AND SECURITY INDEMNIFICATION

In addition to the indemnification provisions in the MOU, the Managed care plan agrees to indemnify, defend, and hold harmless the County, its Special Districts, elected and appointed officers, agents, employees, and volunteers from and against any and all claims, demands liabilities, damages, judgments, awards, losses, costs, expenses or fees including reasonable attorneys' fees, accounting and other expert, consulting or professional fees, and amounts paid in any settlement arising from, connected with, or relating to :

- The Managed care plan's violation of any federal and state laws in connection with its accessing, collecting, processing, storing, disclosing, or otherwise using County Information;

- The Managed care plan's failure to perform or comply with any terms and conditions of this MOU or related agreements with the County; and/or,

- Any Information loss, breach of Confidentiality, or Incident involving any County Information that occurs on the Managed care plan's systems or networks (including all costs and expenses incurred by the County to remedy the effects of such loss, breach of Confidentiality, or Incident, which may include (i) providing appropriate notice to individuals and governmental authorities, (ii) responding to individuals' and governmental authorities' inquiries, (iii) providing credit monitoring to individuals, and (iv) conducting litigation and settlements with individuals and governmental authorities).

Notwithstanding the preceding sentences, the County shall have the right to participate in any such defense at its sole cost and expense, except that in the event managed care plan fails to provide County with a full and adequate defense, as determined by County in its sole judgment, County shall be entitled to retain its own counsel, including, without limitation, County Counsel,

and to reimbursement from managed care plan for all such costs and expenses incurred by County in doing so. Managed care plan shall not have the right to enter into any settlement, agree to any injunction or other equitable relief, or make any admission, in each case, on behalf of County without County's prior written approval.

ADDENDUM A: SOFTWARE AS A SERVICE (SaaS)

a. **License:** Subject to the terms and conditions set forth in this MOU, including payment of the license fees by to the Managed care plan, the Managed care plan hereby grants to County a non-exclusive, non-transferable worldwide County license to use the SaaS, as well as any documentation and training materials, during the term of this MOU to enable the County to use the full benefits of the SaaS and achieve the purposes stated herein.

b. **Business Continuity:** In the event that the Managed care plan's infrastructure containing or processing County Information becomes lost, altered, damaged, interrupted, destroyed, or otherwise limited in functionality in a way that affects the County's use of the SaaS, The Managed care plan shall immediately and within twenty- four (24) hours implement the Managed care plan's Business Continuity Plan, consistent with Section 12 OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY, such that the Managed care plan can continue to provide full functionality of the SaaS as described in the MOU.

   The Managed care plan will indemnify the County for any claims, losses, or damages arising out of the County's inability to use the SaaS consistent with the MOU and Section 18 PRIVACY AND SECURITY INDEMNIFICATION.

   The Managed care plan shall include in its Business Continuity Plan service offering, a means for segmenting and distributing IT infrastructure, disaster recovery and mirrored critical system, among any other measures reasonably necessary to ensure business continuity and provision of the SaaS.

   In the event that the SaaS is interrupted, the County Information may be accessed and retrieved within two (2) hours at any point in time. To the extent the Managed care plan hosts County Information related to the SaaS, the Managed care plan shall create daily backups of all County Information related to the County's use of the SaaS in a segmented or off-site "hardened" environment in a manner that ensures backups are secure consistent with cybersecurity requirements described in this MOU and available when needed.

c. **Enhancements:** Upgrades, replacements and new versions: The Managed care plan agrees to provide to County, at no cost, prior to, and during installation and implementation of the SaaS any software/firmware enhancements, upgrades, and replacements which the Managed care plan initiates or generates that are within the scope of the SaaS and that are made available at no charge to the Managed care plan's other customers.

During the term of this MOU, the Managed care plan shall promptly notify the County of any available updates, enhancements or newer versions of the SaaS and within thirty (30) Days update or provide the new version to the County. The Managed care plan shall provide any accompanying documentation in the form of new or revised documentation necessary to enable the County to understand and use the enhanced, updated, or replaced SaaS.

During the MOU term, the Managed care plan shall not delete or disable a feature or functionality of the SaaS unless the Managed care plan provides sixty (60) Days advance notice and the County provides written consent to delete or disable the feature or functionality. Should there be a replacement feature or functionality, the County shall have the sole discretion whether to accept such replacement. The replacement shall be at no additional cost to the County. If the Managed care plan fails to abide by the obligations in this section, the County reserves the right to terminate the MOU for material breach and receive a pro-rated refund.

d. **Location of County Information:** The Managed care plan warrants and represents that it shall store and process County Information only in the continental United States and that at no time will County Data traverse the borders of the continental United States in an unencrypted manner.

e. **Audit and Certification:** The Managed care plan agrees to conduct an annual System and Organization Controls

(SOC 2 type II) audit or equivalent (i.e. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001:2013 certification audit or Health Information Trust Alliance (HITRUST) Common Security Framework certification audit) of its internal controls for security, availability, integrity, confidentiality, and privacy. The Managed care plan shall have a process for correcting control deficiencies that have been identified in the audit, including follow up documentation providing evidence of such corrections. The results of the audit and the Managed care plan's plan for addressing or resolving the audit findings shall be shared with County's Chief Information Security Officer within ten (10) business days of the Managed care plan's receipt of the audit results. The Managed care plan agrees to provide County with the current audit certifications upon request.

f. **Services Provided by a Submanaged care plan:** Prior to the use of any Submanaged care plan for the SaaS under this MOU, the Managed care plan shall notify County of the proposed submanaged care plan(s) and the purposes for which they may be engaged at least thirty (30) Days prior to engaging the Submanaged care plan and obtain written consent of the County's MOU Administrator.

g. **Information Import Requirements at Termination:** Within one (1) Day of notification of termination of this MOU, the Managed care plan shall provide County with a complete, portable, and secure copy of all County Information, including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in a format to be determined by County upon termination.

h. **Termination Assistance Services:** During the ninety (90) Day period prior to, and/or following the expiration or termination of this MOU, in whole or in part, the Managed care plan agrees to provide reasonable termination assistance services at no additional cost to County, which may include:

i. Developing a plan for the orderly transition of the terminated or expired SaaS from the Managed care plan to a successor;

ii. Providing reasonable training to County staff or a successor in the performance of the SaaS being performed by the Managed care plan;

iii. Using its best efforts to assist and make available to the County any third-party services then being used by the Managed care plan in connection with the SaaS; and

iv. Such other activities upon which the Parties may reasonably agree.

ADDENDUM B: MANAGED CARE PLAN HARDWARE CONNECTING TO COUNTY SYSTEMS

Notwithstanding any other provisions in this MOU, the Managed care plan shall ensure the following provisions and security controls are established for any and all Systems or Hardware provided under this MOU.

a. **Inventory:** The Managed care plan must actively manage, including through inventory, tracking, loss prevention, replacement, updating, and correcting, all hardware devices covered under this MOU. The Managed care plan must be able to provide such management records to the County at inception of the MOU and upon request.

b. **Access Control:** The Managed care plan agrees to manage access to all Systems or Hardware covered under this MOU. This includes industry-standard management of administrative privileges including, but not limited to, maintaining an inventory of administrative privileges, changing default passwords, use of unique passwords for each individual accessing Systems or Hardware under this MOU, and minimizing the number of individuals with administrative privileges to those strictly necessary. Prior to effective date of this MOU, the Managed care plan must document their access control plan for Systems or Hardware covered under this MOU and provide such plan to the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO) for review and approval. The Managed care plan must modify and/or implement such plan as directed by the DISO and CISO.

c. **Operating System and Equipment Hygiene:** The Managed care plan agrees to ensure that Systems or Hardware will be kept up to date, using only the most recent and supported operating systems, applications, and programs, including any patching or other solutions for vulnerabilities, within ninety (90) Days of the release of such updates, upgrades, or patches. The Managed care plan agrees to ensure that the operating system is configured to eliminate any unnecessary applications, services and programs. If for some reason the Managed care plan cannot do so within ninety (90) Days, the Managed care plan must provide a Risk assessment to the County's Chief Information Security Officer (CISO).

d. **Vulnerability Management:** The Managed care plan agrees to continuously acquire, assess, and take action to identify and remediate vulnerabilities within the Systems and Hardware covered under this MOU. If such vulnerabilities cannot be addressed, The Managed care plan must provide a Risk assessment to the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO). The County's CISO must approve the Risk acceptance and the Managed care plan accepts liability for Risks that result to the County for exploitation of any un-remediated vulnerabilities.

e. **Media Encryption:** Throughout the duration of this MOU, the Managed care plan will encrypt all workstations, portable devices (e.g., mobile, wearables, tablets,) and removable media (e.g., portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) associated with Systems and Hardware provided under this MOU in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise required or approved by the County's Chief Information Security Officer (CISO).

f. **Malware Protection:** The Managed care plan will provide and maintain industry-standard endpoint antivirus and antimalware protection on all Systems and Hardware as approved or required by the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO) to ensure provided hardware is free, and remains free of malware. The Managed care plan agrees to provide the County documentation proving malware protection status upon request.

ADDENDUM C: APPLICATION SOURCE CODE REPOSITORY

The Managed care plan shall manage the source code in the manner prescribed in this Addendum unless the MOU prescribes procedures for managing the source code and those procedures are no less stringent than the procedures described in this addendum.

a. **County Application Source Code**. To facilitate the centralized management, reporting, collaboration, and continuity of access to the most current production version of application source code, all code, artifacts, and deliverables produced under this MOU, (hereinafter referred to as "County Source Code") shall be version controlled, stored, and delivered on a single industry-standard private Git repository, provided, managed, and supported by the County. Upon commencement of the MOU period, the Managed care plan will be granted access to the County's private Git repository.

b. **Git Repository.** The Managed care plan will use the County Git repository during the entire lifecycle of the project from inception to final delivery. The Managed care plan will create and document design documents, Data flow diagrams, security diagrams, configuration settings, software or hardware requirements and specifications, attribution to third-party code, libraries and all dependencies, and any other documentation related to all County Source Code and corresponding version-controlled documentation within the Git repository. This documentation must include an Installation Guide and a User Guide for the final delivered source code such that County may download, install, and make full functional use of the delivered code as specified and intended.