MEMORANDUM OF

UNDERSTANDING BETWEEN

ORANGE COUNTY HEALTH AUTHORITY, A PUBLIC AGENCY, DBA CALOPTIMA HEALTH

AND

COUNTY OF ORANGE CALIFORNIA CHILDREN'S SERVICES WHOLE CHILD

MODEL PROGRAM

I PURPOSE

The purpose of this Memorandum of Understanding ("**MOU**") between **County of Orange through its agency, the Orange County Health Care Agency, a political subdivision of the State of California** ("**County**"), and **Orange County Health Authority, a public agency dba CalOptima Health** ("**MCP**") (both collectively referred to as the "**Parties**" or individually as a "**Party**") is to identify each Party's responsibilities and obligations to each other in accordance with and based on Health and Safety Code ("**H&S Code** section 123800 *et seq*., statutory requirements related to administration of the California Children's Services ("**CCS**") Program by local county programs, the MCP's respective contract with the Department of Health Care Services ("**DHCS**"), and all other applicable authorities. This MOU outlines the respective roles of the County and the MCP to coordinate care, conduct administrative activities, and engage in information exchange activities required for the effective and seamless delivery of CCS services to CCS eligible individuals enrolled with MCP ("**Members**"). This MOU is a binding contractual agreement. This MOU replaces and terminates any other prior MOUs between the Parties regarding coordination of services between MCP and County for the CCS Whole Child Model ("**WCM**") program.

The County and/or DHCS will retain all administrative responsibilities of case management, care coordination, provider referral, and service authorization functions of the CCS Program as it pertains to CCS State-only Members or Members that are currently in Fee for Service Medi-Cal.

II TERM

This MOU is in effect as of November 1, 2024 ("**Effective Date**") and continues for a term of three (3) years.

III DHCS APPROVAL

MCPs must submit all fully executed MOUs to their Managed Care Operations Division Contract Manager for file and use. In their submissions, MCPs must attest that they did

not modify any of the provisions of this MOU Template except to add provisions that do not conflict with or reduce either Party's obligations under this MOU Templates. If the MCP or County modifies any of the provisions of the MOU Template, the MCP must submit a redlined version of the MOU to DHCS for review and approval, prior to execution.

The Parties must review the MOU annually thereafter to determine whether any modifications, amendments, updates, or renewals of responsibilities and obligations outlined within are required. The MCP must provide evidence to DHCS of the annual review of MOU as well as copies of any MOU modified or renewed as a result. The evidence of the annual review described in the annual report must include a summary of the review process and outcomes, and any resulting amendments to the MOU or existing policies and procedures.

IV CONFIDENTIALITY

All responsibilities and information shared by the County and the MCP in the provision of services for CCS eligible Members and under this MOU must adhere to all applicable Federal, State and/or local laws and regulations relating to confidentiality of the information subject to the performance of this MOU.

V LIABILITY AND INDEMNITY

County and the MCP are not liable to third parties for any act or omission of the other Party. Each Party is solely liable for any negligent or wrongful acts or omissions of its own officers, agents, and employees occurring in the performance of this MOU. If either the County or the MCP is held liable by a court of competent jurisdiction for damages caused by its officers, agents or employees, it must pay such damages without contribution by the other Party and hold harmless the other Party from all costs and expenses resulting from any attorney fees and court costs, claims, losses, damages, and liabilities.

VI RECORDS, AUDITS & INSPECTIONS

County and the MCP must at any time, upon reasonable notice during business hours and as necessary, make all of its records and data with respect to the matters covered by this MOU and the CCS Program available for examination by local, state, or federal authorities, pursuant to applicable state or federal statute or regulation. The MCP must retain all documents demonstrating compliance with this MOU for at least ten (10) years. The MCP must post this executed MOU on its website. The County may post this executed MOU on its website.

VII SCOPE OF RESPONSIBILITIES

The table below identifies the roles and responsibilities of each Party as they relate to providing CCS services to CCS Eligible Members, including Eligibility and Enrollment Services, Case Management Services, Intercounty Transfers ("**ICT**"), CCS Advisory

Committees, Continuity of Care, Data and Information Sharing, Emergency Preparedness, Dispute Resolution, Neonatal Intensive Care Unit ("**NICU**") Services, Quality Assurance and Monitoring, and Subcontractors. Not all CCS applicable regulations or other requirements are listed in the table below.

CCS Eligible Member Eligibility and Enrollment (Case Identification and Referral)	
MCP	**County**
The MCP must provide necessary documentation, including but not limited to medical records/case notes/reports pertaining to the CCS-eligible condition, to the County to assist with initial and annual medical eligibility determinations. The MCP must refer a Member to the County for a CCS eligibility determination if the Member demonstrates a potential CCS condition(s) as outlined in the CCS Medical Eligibility Guide, which may be amended. The MCP must include supporting documentation of the Member's potential CCS eligible condition in all of its CCS referrals to the County. MCPs will be responsible for conducting the CCS NICU eligibility criteria assessment, authorization, and payment. Upon notification from the County, the MCP must obtain and provide to the county any additional information the County requires, such as medical reports pertaining to the CCS-eligible condition, to make a CCS Program eligibility determination. Within ninety (90) days of its referral to the County, the MCP must inform the CCS eligible Member and their family (or designated legal caregiver) about the availability of medical care related to the CCS eligible condition. MCP must provide training and orientation for its employees, Network Providers, Subcontractors, and Downstream	Independent counties are responsible for medical, financial, and residential eligibility determinations for referred CCS members, including determining initial medical eligibility determinations and redeterminations. Dependent counties are responsible for determining financial and residential eligibility. DHCS is responsible for determining medical eligibility for new referrals and annual redeterminations; except for NICU and High Risk Infant Follow-Up ("**HRIF**") eligibility determinations. The County must inform the child (Member under age 21) and their family (or designated legal caregiver) of the CCS Program eligibility determination. The County must inform the child determined to be ineligible and their family (or designated legal caregiver) of the CCS Program eligibility appeal process. The County must communicate to the MCP the CCS Program eligibility determination. The County must request any additional information required (*e.g.,* medical reports) to make a program eligibility determination from the MCP. The County must provide notification to the MCP when the county becomes aware the member has moved out of the

CCS Eligible Member Eligibility and Enrollment (Case Identification and Referral)	
MCP	**County**
Subcontractors who carry 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. The MCP must provide the training prior to any such person or entity performing responsibilities under this MOU, and at least annually thereafter. The MCP must require its Subcontractors and Downstream Subcontractors to provide training on relevant MOU requirements and the County's programs and services to its Network Providers. The MCP must provide educational materials to its Members and Network Providers related to accessing Medically Necessary Services, including materials provided by the County. The MCP must provide County with training and/or educational materials on how MCP Covered Services may be accessed, including during nonbusiness hours. The MCP must provide medical records to the County for the annual medical review ("**AMR**") of CCS Program eligibility, including the most current medical records that document the CCS eligible Member's medical history; the results of a physical examination by a physician; and laboratory test results, radiologic findings, or other tests or examinations that support the diagnosis of the eligible condition(s). The MCP's documentation must be dated within six (6) months before the Member's program eligibility end date, to the extent possible, but no later than twelve (12) months before the Member's program eligibility end date.	county. The County must proactively engage in a collaborative process with the MCP to remedy any issues or challenges related to timeliness or completeness of records for the medical eligibility redetermination process. The County must request medical records from the MCP for the annual medical review three (3) months in advance of the member's program eligibility end date. The County must notify the MCP when the County becomes aware that a CCS Eligible Member has lost Medi-Cal eligibility.

CCS Eligible Member Eligibility and Enrollment (Case Identification and Referral)	
MCP	**County**
The MCP must provide the documentation set forth above to the County sixty (60) calendar days before the Member's program eligibility end date. If documentation is received by the County outside of the agreed upon timeframe, the MCP and County must collaborate to determine the best approach and time frame for submitting the required documentation. If appointments occur within the sixty (60) calendar day period prior to the Member's program eligibility end date, the MCP and County must have procedures in place to ensure all appropriate most recent medical records that document the Member's medical history, results of a physical examination by a physician or an advanced practiced provider acting within the scope of their licensing authority, laboratory test results, radiologic findings, or other tests or examinations that support the diagnosis of the eligible condition(s), including any Medical Therapy Program ("**MTP**") diagnosis are submitted to support AMR. If the County requires additional documentation, the MCP must, upon notification from the County, coordinate with the Member's provider(s) to obtain documentation, before the Member's CCS Program eligibility end date. The MCP must have procedures in place regarding outreach attempts to providers and the CCS member to obtain medical records, as well as appropriate actions to take if the MCP's efforts to obtain medical records are unsuccessful. The MCP must provide notification and necessary documentation to the County to assist with transition from MCP to CCS-State Only.	

CCS Eligible Member Eligibility and Enrollment (Case Identification and Referral)	
MCP	**County**
The MCP must notify the County when the MCP becomes aware that a CCS eligible Member has lost Medi-Cal eligibility. The MCP must proactively engage in a collaborative process with the County to remedy any issues or challenges related to timeliness or completeness of records for the medical eligibility redetermination process.	

Case Management (Care Coordination)	
MCP	**County**
The MCP must refer Members to the County if these Members are suspected of having an **MTP** eligible condition and must include all supporting documentation with the referral. As a part of the CCS eligibility review, the County will review and determine MTP eligibility, if applicable. MCP must ensure that a CCS-eligible child has a primary point of contact who shall be responsible for the child's care coordination. The MCP must coordinate with the local CCS Medical Therapy Unit ("**MTU**") to ensure appropriate access to MTP services. The MCP must consult with county MTP to coordinate durable medical equipment ("**DME**") equipment needs of MTP eligible clients, as necessary. The MCP must not duplicate therapy services rendered by an MTP. The MCP must notify the County of CCS eligible neonates, infants, and children up to three (3) years of age that lose Medi-Cal	The CCS County Administrator or designee must coordinate with the MCP liaison or the MCP Utilization Management Director regarding member enrollment, as often as necessary. The County must submit referrals to the MCP for medically necessary specialty services and follow-up treatment, as prescribed by the County's Medical Therapy Conference ("**MTC**") team physician. The County MTP is responsible for the provision of medically necessary occupational and physical therapy services prescribed by the County CCS MTU Conference Team Physician or the CCS-paneled physician who is providing the medical direction for occupational and physical therapy services. Upon notification from the MCP of a CCS Member that has lost MCP coverage, the County must ensure the coordination of HRIF outpatient diagnostic services. The County must regularly communicate,

Case Management (Care Coordination)	
MCP	**County**
coverage for HRIF services. The MCP must regularly communicate and share relevant information via telephone and/or case management notes, written or electronic, with the County to facilitate the care of CCS Members who require services from both the County and the MCP. Communication may be via telephone, written, electronic case management notes, or secure email. The MCP must provide CCS Maintenance and Transportation ("**M&T**") and Non-Medical Transportation ("**NMT**") for all Medically Necessary Covered Services, including services provided through the CCS Program and MTP, and coordinate Non-Emergency Medical Transportation ("**NEMT**"). The MCP must ensure reimbursements for M&T expenses are available to the CCS eligible Member or their family in accordance with CCS Numbered Letter ("**NL**") 03-0810 and All Plan Letter ("**APL**") 21-005 or any superseding version of this NL and APL. The MCP must provide and authorize the CCS M&T benefit for CCS eligible Members or the Member's family seeking transportation to a medical service related to their CCS eligible condition(s) when the cost of M&T presents a barrier to accessing authorized CCS services. The MCP must authorize services based on medical necessity and/or evidence- based guidelines, including DME, consistent with CCS program standards. The MCP must ensure all services related to the Member's CCS eligible condition are provided by either CCS-paneled providers, CCS-approved Special Care Centers ("**SCCs**"), and/or CCS- approved pediatric acute care	share relevant information via telephone and/or case management notes, written or electronic, with the MCP to facilitate the care of CCS WCM Members who require MTP services. Communication may be via telephone, written, electronic case management notes, or secure email. The County must identify staff who will meet quarterly and more often as necessary with the appointed MCP Liaison(s).

Case Management (Care Coordination)	
MCP	**County**
hospitals. The MCP must provide case management services for CCS eligible conditions, to coordinate benefits, and to authorize services according to state regulations and APL 21-005 or any superseding APL. The MCP must inform CCS eligible Members of the availability of the CCS program and benefits as needed. The MCP must authorize a CCS paneled provider or center to treat and manage the CCS eligible condition. The MCP must, as part of its provider education strategy, educate Network Providers about the local CCS Program and the ways that the Primary Care Physician ("**PCP**") can assist with integration of CCS authorized services. The MCP must ensure that CCS eligible Members receive all Medically Necessary pediatric preventive services, including immunizations, unless determined to be medically contraindicated. MCP must authorize, refer, and coordinate the delivery of Organ and Bone Marrow Transplant benefits and all Medically Necessary Covered Services associated with a transplant service. MCP must ensure that organ and bone marrow transplants services are provided to the Member at a CCS-approved SCC that has current CCS approval to transplant the specified organ in the Member's age group in accordance with Attachment 2 of APL 21-015 or any superseding APL. The MCP must conduct a HRIF program	

Case Management (Care Coordination)	
MCP	**County**
acuity assessment and authorize any HRIF services for the Member in accordance with the HRIF Eligibility Criteria. The MCP must ensure access or arrange for the provision of HRIF case management services. The MCP must notify the County of any CCS eligible neonates, infants, and children up to three (3) years of age that have been identified as having a potential CCS eligible condition through the HRIF program. The MCP must accompany any referral to the County with supporting documentation of the Member's potential CCS eligible condition. The MCP must develop and implement policies and procedures (P&Ps) that specify coordination activities and communication requirements among PCPs, specialty providers, hospitals, and the assigned case manager(s). The MCP must ensure that CCS eligible Members and their families have ongoing information, education, and support regarding: • How to request continuity of care for pharmacy, specialized DME, and health care providers; • How to request M&T services; • How to request assistance with the transition to adult care; • Referrals to community resources; • The child's and family's role in the individual care process; • The availability of mental health services; and • Any other services that might be available (*i.e.* Regional Centers and Home and Community Based	

Case Management (Care Coordination)	
MCP	**County**
Alternatives Waiver Agencies) The MCP must determine which staff will be appropriate to meet, at a minimum quarterly and as often as necessary, and maintain communication with the appointed CCS Liaison(s).	

Intercounty Transfer (ICT)	
MCP	**County**
The MCP must complete its ICT form and provide the County with the following documentation no later than ten (10) working days when requested by the County for a CCS eligible Member's ICT: • Copies of current physical medical reports since the most recent annual medical redetermination. The MCP is not required to send reports from MTC. • A list of the Member's authorized providers from at least the previous twelve (12) months. • A list of the Member's authorized services from at least the previous twelve (12) months. • Any information that will assist the Receiving County of residence or receiving MCP in making authorization decisions. • Case management notes related to the CCS eligible medical condition, if possible. If that is not possible, the MCP must provide a summary note of relevant case management activities. During an ICT, the MCP must continue to provide case management services and	During an ICT, the County must forward to a Member's new county of residence a completed ICT form and any documentation that the County received from the MCP. When the Member in the Sending County is enrolled in a WCM MCP, the Sending County must request the most recent medical reports, case management notes, and utilization information from the WCM MCP. The Receiving County is encouraged to collaborate with the MCP during their negotiations of a transfer date with the Sending County. For further guidance on ICTs, refer to the CCS Intercounty Transfer NL 09-1215. County must follow CCS Intercounty Transfer Policy NL 09-1215 or any superseding version of this NL.

Intercounty Transfer (ICT)	
MCP	**County**
make determinations as to Medically Necessary service authorization requests until the Member's transfer date. The MCP must coordinate with the County regarding the ICT date. The MCP must authorize Out-of-Network requests if the Member requires services in their new county of residence prior to the transfer date. During an ICT, the MCP must close all service authorization requests at least the day before the transfer date. The MCP must follow CCS ICT guidance in accordance with CCS Intercounty Transfer NL 09-1215 or any superseding NL.	

CCS Advisory Committees (Clinical Advisory and Family Advisory)	
MCP	**County**
The MCP must create and maintain a Clinical Advisory Committee composed of: • The MCP's medical director or the equivalent; • The County's CCS administrator, medical director or designee; • At least four CCS-paneled providers; and • The County's CCS Liaison(s) The Clinical Advisory Committee must meet at least quarterly or more frequently if determined to be necessary. The MCP's Family Advisory Committee ("**FAC**") must ensure meaningful	The following County representatives must actively participate in the MCP's Clinical Advisory Committee: • The County's CCS administrator; medical director or designee; or • The County's CCS Liaison The County's representatives will actively participate by: • Attending meetings; • Engaging in discussion; and • Offering feedback and recommendations. The County must collaborate with the MCP

CCS Advisory Committees (Clinical Advisory and Family Advisory)	
MCP	**County**
engagement of its members, which must include: • The County's CCS Liaison(s); • The County's CCS representative(s); and • CCS provider representatives. The MCP must coordinate with the County's CCS staff, local CCS providers, and consumer advocates to recruit CCS families for the FAC. The MCP must coordinate with CCS families to ensure they understand the FAC's role and their role as members of the FAC. The MCP may provide a reasonable per diem payment to enable in-person participation in the advisory committee. The MCP may utilize teleconference or other similar electronic means to facilitate participation.	to ensure meaningful engagement with family members. The County must coordinate with the MCP, local CCS providers, and consumer advocates to assist in recruiting CCS families for the FAC. The County must coordinate with CCS families to ensure they understand the FAC's role and their role as members of the FAC.

A. Continuity of Care	
MCP	**County**
Upon transitioning to WCM: If requested by the CCS eligible Member within ninety (90) days of the transition of their CCS services to the MCP, the MCP must ensure that the CCS eligible Member continues to receive case management and care coordination from their public health nurse ("**PHN**"), if the PHN is available and the County and MCP reach a mutually agreeable financial arrangement. The MCP must establish and maintain a process by which a CCS eligible Member may maintain access to navigating a health plan; maintain rights to appeal any service denials; and request COC for pharmacy, health care providers, and specialized or customized DME providers for up to twelve (12) months. The MCP must ensure that CCS families have ongoing information, education, and support regarding the rights to appeal any service denials, including the right to appeal a denial of **COC** beyond twelve (12) months, in accordance with APL 21-005, APL 22-032 or any superseding APLs. The MCP must attempt to enter into a Letter of Agreement ("**LOA**") with the provider to allow for COC for at least one (1) year if the child has established care with	Upon transitioning to WCM; The County must respond to the MCP within two (2) working days regarding the CCS eligible Member's request to continue working with their PHN. In the event that the requested PHN is no longer available, the County must provide reasonable notice to the MCP of the PHN's last day in the CCS Program. If the County does not want to proceed with discussions, the County must submit a written notification to DHCS and MCP on county letterhead to advise on the decision. The County must provide information on active CCS eligible Member cases to the MCP unless a case has already been transitioned. The County is primarily responsible for providing case management to arrange all approved Private Duty Nursing ("**PDN**") service hours if the County approves the PDN services for a CCS eligible Member under the age of twenty-one (21). Existing WCM Counties must coordinate COC services with the MCP to the extent possible to ensure no delays of services to members. The County must follow Continuity of Care guidance in accordance with H&S Code Section 123850(b).

A. Continuity of Care	
MCP	**County**
a provider prior to WCM and if that provider is not contracted with the MCP. The MCP is primarily responsible for providing case management to arrange all approved PDN service hours if the MCP approves the PDN services for a Medi-Cal eligible CCS Member under the age of twenty-one (21) If CCS has authorized PDN services and is primarily responsible for providing case management for those PDN services, MCP must still provide case management as necessary, including, at Member's request, arranging for all approved PDN services as required by APL 20-012 or any superseding APL.	

Data and Information Sharing (HIPAA/Medical Records Sharing)	
MCP	**County**
The MCP must ensure any Subcontractors or Network Providers that create, receive, maintain, or transmit protected health information on behalf of the MCP agree to the same privacy restrictions, conditions, and requirements that apply to the MCP. The MCP must ensure that appropriate staff has access to the Children's Medical Services Provider Electronic Data Interchange ("**PEDI**") to view the status of CCS Eligible Member data. The MCP must, in collaboration with the County, 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	The County must ensure any Providers that create, receive, maintain, or transmit protected health information on behalf of the County agree to the same privacy restrictions, conditions, and requirements that apply to the County. The County must ensure any Subcontractors that create, receive, maintain, or transmit protected health information on behalf of the County CCS Program agree to the same restrictions, conditions, and requirements that apply to the County. The County must, in collaboration with MCP, implement policies and procedure to ensure that the minimum necessary Member information and data for accomplishing the goals of this MOU and are exchanged timely and maintained securely and confidentially and in

Data and Information Sharing (HIPAA/Medical Records Sharing)	
MCP	**County**
below. The MCP and County must share information in compliance with applicable law, which may include the Health Insurance Portability and Accountability Act and its implementing regulations at 45 C.F.R. Parts 160 and 164, as they may now exist or may be hereafter amended ("**HIPAA**"), Part 2 of Title 42 of the Code of Federal Regulations (C.F.R.), and any other applicable State of California ("**State**") and federal privacy laws. The MCP must attach these P&Ps to this MOU within ninety (90) calendar days of execution of this MOU.	compliance with the requirements set below. The MCP and County must share information in compliance with applicable law, which may include HIPAA, as amended, 42 C.F.R. Part 2, and other State and federal privacy laws. These policies and procedures must be attached to this MOU within ninety (90) calendar days of execution.

Dispute Resolution	
MCP	**County**
If there is a dispute between the MCP and the County, all parties are responsible for carrying out all their responsibilities under the MOU without delay, including providing Members with access to services under the MOU. The MCP must designate appropriate staff to participate in dispute resolution with the County. The MCP must meet at least quarterly with the County's CCS liaison(s) and the County's staff regarding operational and administrative issues. The MCP must respond timely to the County's dispute resolution requests. Disputes between the MCP and the County regarding CCS medical eligibility determinations that cannot be reached by mutual agreement in a good faith attempt between the MCP and the County must be forwarded by either	If there is a dispute between the County and the MCP, all parties are responsible for carrying out all their responsibilities under the MOU without delay, including providing Members with access to services under the MOU. The County must designate appropriate staff to participate in dispute resolution with the MCP. The County must meet at least quarterly with the MCP's Program/liaison staff regarding operational and administrative issues. The County must communicate all resolved disputes in writing to the MCP. Disputes between the County and the MCP regarding CCS medical eligibility determinations that cannot be resolved in a good faith attempt between the MCP and the County must be forwarded by either Party to DHCS via email to CCSRedesign@dhcs.ca.gov for review and a final determination.

Dispute Resolution	
MCP	**County**
Party to DHCS via email to CCSRedesign@dhcs.ca.gov for review and a final determination.	

Neonatal Intensive Care Unit (NICU)	
MCP	**County**
The MCP must conduct assessments in accordance with CCS Program guidelines for medical eligibility for care in a CCS-approved NICU, as found in CCS NL 05-0502 or any superseding NL. In order to capture the CCS referral, the MCP must report to the County's CCS Program all Members identified as meeting the criteria for the NICU eligibility assessment. The MCP must accompany any CCS referral to the County with supporting documentation of the Member's potential CCS eligible condition.	The County must review all cases for CCS Program determinations referred to the County by an MCP when a Member may have any newly identified or potential CCS-eligible conditions, including infants with a potential CCS-eligible condition at time of discharge from the NICU, as well as infants and children undergoing diagnostic evaluation for CCS-eligible conditions.

Quality Assurance and Monitoring	
MCP	**County**
MCP must collaborate with the County to establish policies and procedures for oversight of all of the requirements of this MOU, including, without limitation, requirements related to combined Quality Improvement ("**QI**") activities, including, but not limited to, any applicable performance measures and QI initiatives as well as reports that track cross-system referrals, CCS eligible Member engagement, and service utilization and to prevent duplication of services rendered.	The County must collaborate with the MCP to establish policies and procedures for oversight of all of the requirements of this MOU, including, without limitation, requirements related to QI activities, including, but not limited to, any applicable performance measures and QI initiatives as well as reports that track cross-system referrals, CCS eligible Member engagement, and service utilization and to prevent duplication of services rendered.

Quality Assurance and Monitoring	
MCP	**County**
The MCP must participate in meetings with the County at least quarterly to update P&Ps and protocols as appropriate. The MCP and the County may establish frequency of meetings. • All documentation related to these meetings should be made available to DHCS for auditing purposes, including agendas and sign-in sheets. Meeting facilitation is determined by the MCP and the County. The MCP's CCS liaison must report to the MCP's Compliance Officer on the MCP's compliance with the MOU no less frequently than quarterly	Meeting facilitation is determined by the County and MCP.

Subcontractors	
MCP	**County**
The MCP must ensure that all of its Subcontractors comply with all California Welfare and Institutions Code Section 123850 requirements that apply to the MCP.	The County must ensure that all of its Subcontractors comply with all California Welfare and Institutions Code Section 123850 requirements that apply to the County.

VIII AMENDMENTS

The County and the MCP may amend this MOU at any time by written, mutual consent. The County and the MCP must submit any proposed amendments to this MOUs to DHCS and receive DHCS' final review and approval before execution of the amended MOU.

IX LIAISONS

The MCP must designate an individual or set of individuals as part of its Provider Relations/Community Relations or related functions to serve as the liaison for CCS county administrators and providers, including CCS specialty care center providers.

The County and the MCP must designate CCS liaisons to be the primary points of contact for this MOU. The CCS liaisons must meet no less than quarterly to discuss activities related to this MOU and any other related matters. The County and the MCP must also submit the contact information for their respective liaisons to DHCS.

For the purposes of this MOU, the primary liaison for the MCP is the Hannah Kim, Director of Case Management and the primary liaison for the County is the [Doris Billings, BS, PBACC, OT/L, Medical Services Manager, Senior; Program Manager California Children's Services or delegate as specified by the County Director.

X DATA INFORMATION SHARING AGREEMENT(S)

The purpose of this Section X is to ensure the protection of any data or information shared between the Parties related to the WCM in accordance with HIPAA and any other applicable State and/or federal privacy laws related to the confidentiality and security of WCM information. The Parties agree to comply with Exhibit A, Business Associate Agreement, to ensure protection of any data or information shared between the Parties related to the WCM in accordance with HIPAA and any other applicable State and/or federal privacy laws related to the confidentiality and security of WCM information.

DocuSigned by:
Dr. Veronica Kelley 11/4/2024
E8B80965A4EC417...

Health and Human Services or Public Health Department Director **Date**

Signed by:
Doris Billings Oct 25, 2024
897E34267EB24C7...

CCS County Administrator **Date**

M Hunn Oct 25, 2024
Michael Hunn (Oct 25, 2024 13:48 PDT)

MCP Chief Executive Officer **Date**

Exhibit A – Business Associate Agreement

This Exhibit A shall only apply if one Party is acting as a business associate (as that term is defined in 45 C.F.R. § 160.103) of the other Party. References to "**Covered Entity**" in this Exhibit A shall refer to County when MCP is acting as the County's Business Associate and shall refer to MCP when County is acting as the MCP's Business Associate. References to "**Business Associate**" in this Exhibit A shall refer to County when County is acting as a Business Associate to MCP and shall refer to MCP when MCP is acting as a Business Associate to County.

1. **Definitions.** The terms in this section and otherwise defined in this Business Associate Agreement shall have the definitions set forth below for purposes of this Business Associate Agreement. Terms used, but not otherwise defined, in this Business Associate Agreement shall have the same meaning as those terms in HIPAA, the HITECH Act, the IPA (as defined below), and/or regulations promulgated thereunder.

a. **Agreement** as used in this document means both this Business Associate Agreement and the MOU to which this Business Associate Agreement applies.

b. **Breach** means, unless expressly excluded under 45 C.F.R. § 164.402, the acquisition, access, Use, or Disclosure of PHI in a manner not permitted under Subpart E of 45 C.F.R. Part 164 which compromises the security or privacy of the PHI and as more particularly defined under 45 C.F.R. § 164.402.

c. **Business associate** has the meaning given such term in 45 C.F.R. § 160.103.

d. **Confidential Information** refers to information not otherwise defined as PHI in Section 1(o) below, but to which state and/or federal privacy and/or security protections apply.

e. **Data Aggregation** has the meaning given such term in 45 C.F.R. § 164.501.

f. **Designated Record Set** has the meaning given such term in 45 C.F.R. § 164.501.

g. **Disclose** and **Disclosure** mean the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

h. **Electronic Health Record** has the meaning given such term in 42 U.S.C. § 17921.

i. **Electronic Media** means:

i. Electronic storage material on which data is or may be recorded electronically including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

ii. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet, extranet or intranet,

leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via Electronic Media, because the information being exchanged did not exist in electronic form before the transmission.

j. **Electronic Protected Health Information** ("**ePHI**") means Individually Identifiable Health Information, including PHI, that is transmitted by or maintained in Electronic Media.

k. **Health Care Operations** has the meaning given such term in 45 C.F.R. § 164.501.

l. **Individual** means the person who is the subject of PHI and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

m. **Individually Identifiable Health Information** means health information, including demographic information collected from an Individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an Individual, the provision of health care to an Individual, or the past, present, or future payment for the provision of health care to an Individual, that identifies the Individual or where there is a reasonable basis to believe the information can be used to identify the Individual, as set forth under 45 C.F.R. § 160.103.

n. **Information System** means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

o. **Protected Health Information** ("**PHI**"), as used in this Agreement and unless otherwise stated, refers to and includes both PHI as defined at 45 C.F.R. § 160.103 and personal information ("**PI**") as defined in the Information Practices Act at California Civil Code § 1798.3(a) ("**IPA**"). PHI includes information in any form, including paper, oral, and electronic.

p. **Reproductive Health Care** means health care, as defined at 45 C.F.R. § 160.103, that affects the health of an Individual in all matters relating to the reproductive system and to its functions and processes.

q. **Required by Law** means a mandate contained in law that compels an entity to make a Use or Disclosure of PHI and that is enforceable in a court of law. Required by Law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing benefits.

r. **Secretary** means the Secretary of the U.S. Department of Health and Human Services or the Secretary's designee.

s. **Security Incident** means the attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of information or interference with system operations in an Information System.

t. **Services** mean those services contemplated by the MOU.

u. **Unsecured Protected Health Information** ("**Unsecured PHI**") means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under 42 U.S.C. § 17932(h)(2).

v. **Use** and **Uses** mean, with respect to Individually Identifiable Health Information, the sharing, employment, application, utilization, examination or analysis of such information within the entity that maintains such information.

2. Covered Entity intends that Business Associate may create, receive, maintain, transmit or aggregate certain information pursuant to the terms of this Agreement, some of which information may constitute PHI and/or Confidential Information protected by federal and/or state laws.

3. Business Associate is the business associate of Covered Entity acting on Covered Entity's behalf and provides services or arranges, performs or assists in the performance of functions or activities on behalf of Covered Entity, and may create, receive, maintain, transmit, aggregate, Use or Disclose PHI in order to fulfill Business Associate's obligations under this Agreement.

4. **Permitted Uses and Disclosures of PHI by Business Associate.** Except as otherwise indicated in this Agreement, Business Associate may Use or Disclose PHI, inclusive of de-identified data derived from such PHI, only to perform functions, activities or services specified in this Agreement on behalf of Covered Entity, provided that such Use or Disclosure would not violate HIPAA, including the Privacy Regulations, or other applicable laws if done by Covered Entity.

a. **Specific Use and Disclosure Provisions.** Except as otherwise indicated in this Agreement, Business Associate may Use and Disclose PHI if necessary for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate. Business Associate may Disclose PHI for this purpose if the Disclosure is Required by Law, or the Business Associate obtains reasonable assurances, in writing, from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware that the confidentiality of the information has been breached, unless such person is a treatment provider not acting as a business associate of Business Associate.

b. **Data Aggregation.** If authorized as part of the Services provided to Covered

Entity under the MOU, Business Associate may use PHI to provide Data Aggregation services relating to the Health Care Operations of Covered Entity.

5. **Prohibited Uses and Disclosures of PHI.**

a. **Restrictions on Certain Disclosures to Health Plans.** Business Associate shall not Disclose PHI about an Individual to a health plan for payment or Health Care Operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the Individual requests such restriction in accordance with HIPAA and the HITECH Act, including 45 C.F.R. § 164.522(a). The term PHI, as used in this Section, only refers to PHI as defined in 45 C.F.R. § 160.103.

b. **Prohibition on Sale of PHI; No Remuneration.** Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written authorization of Covered Entity and Covered Entity's regulator(s), as applicable, and then, only as permitted by HIPAA and the HITECH Act. The term PHI, as used in this Section, only refers to PHI as defined in 45 C.F.R. § 160.103.

c. **Prohibition of Disclosure of PHI Related to Reproductive Health Care**. Business Associate shall comply with 45 C.F.R. Part 164, Subpart E regarding uses and disclosures of Reproductive Health Care-related information, including the following:

i. Business Associate shall comply with requirements of 45 § C.F.R. 164.502(a)(5)(iii) and shall not Use or Disclose PHI related to lawful Reproductive Health Care for the purpose of (i) conducting a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating Reproductive Health Care; (ii) imposing criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating Reproductive Health Care; or (iii) to identify any person for any purpose previously described (each a "**Prohibited Purpose**").

ii. To the extent applicable, if Business Associate receives a request for Reproductive Health Care-related information for a non-Prohibited Purpose that is otherwise permissible under HIPAA, HITECH, the Privacy Regulations, and the Security Regulations, Business Associate shall obtain a valid attestation under 45 C.F.R. § 164.509 if the requested release of Reproductive Health Care-related information is for: (i) health oversight activities under 45 C.F.R. § 164.512(d); (ii) judicial or administrative proceedings under 45 C.F.R. § 164.512(e); (iii) disclosures for law enforcement purposes under 45 C.F.R. § 164.512(f); or (iv) disclosures about decedents to coroners and medical examiners under 45 C.F.R. § 164.512(g)(1).

6. **Compliance with Other Applicable Laws.**

a. To the extent that other state and/or federal laws provide additional, stricter and/or more protective (collectively, "more protective") privacy and/or security protections to PHI or other Confidential Information covered under this Agreement beyond those provided through HIPAA, Business Associate agrees:

i. To comply with the more protective of the privacy and security standards

set forth in applicable state or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the Individuals whose information is concerned; and

ii. To treat any violation of such additional and/or more protective standards as a Breach or Security Incident, as appropriate, pursuant to Section 17 of this Agreement.

b. Examples of laws that provide additional and/or stricter privacy protections to certain types of PHI and/or Confidential Information, as defined in Section 1 of this Agreement, include, but are not limited to the IPA (*i.e.*, California Civil Code §§ 1798-1798.78), CMIA (*i.e.*, California Civil Code Section 56 *et seq*.), Confidentiality of Alcohol and Drug Abuse Patient Records (*i.e.*, 42 C.F.R. Part 2), Welfare and Institutions Code §§ 5328 through 5329, and California Health and Safety Code § 11845.5. Business Associate shall ensure that any Medical Information related to Sensitive Services (as those terms are defined under Civil Code § 56.05) received or accessed under this Agreement is kept confidential, segregated, and only disclosed, accessed, transferred, transmitted, or processed in accordance with CMIA requirements, including Civil Code §§ 56.10, 56.11, 56.107, 56.108, and 56.110, as applicable.

c. If Business Associate is a Qualified Service Organization ("**QSO**") as defined in 42 C.F.R. § 2.11, Business Associate agrees to be bound by and comply with subdivisions (2)(i) and (2)(ii) under the definition of QSO in 42 C.F.R. § 2.11.

7. **Additional Responsibilities of Business Associate.**

a. **Nondisclosure.** Business Associate shall not Use or Disclose PHI or other Confidential Information other than as permitted or required by this Agreement or as Required by Law.

b. **Safeguards and Security.**

i. Business Associate shall use safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI and other confidential data and comply, where applicable, with Subpart C of 45 C.F.R. Part 164 with respect to ePHI, to prevent Use or Disclosure of the information other than as provided for by this Agreement. Such safeguards shall be, at a minimum, at Federal Information Processing Standards (FIPS) Publication 199 protection levels. Business Associate shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of Subpart C of 45 C.F.R. Part 164, in compliance with 45 C.F.R. § 164.316. Business Associate shall maintain a comprehensive written information privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its activities.

ii. Business Associate shall, at a minimum, utilize National Institute of Standards and Technology Special Publication (NIST SP) 800-53 compliant security framework when selecting and implementing its security controls, and shall maintain continuous compliance with NIST SP 800-53 as it may be updated from time to time.

iii. Business Associate shall employ FIPS 140-3 compliant encryption of PHI at rest and in motion unless Business Associate determines it is not reasonable and appropriate to do so based upon a risk assessment, and equivalent alternative measures are in place and documented as such. Business Associate shall maintain, at a minimum, the most current industry standards for transmission and storage of PHI and other Confidential Information, including, but not limited to, encryption of all workstations, laptops, and removable media devices containing PHI and data transmissions of PHI.

iv. Business Associate shall apply security patches and upgrades, and keep virus software up-to-date, on all systems on which PHI and other Confidential Information may be used.

v. Business Associate shall ensure that all members of its workforce with access to PHI and/or other Confidential Information sign a confidentiality statement prior to access to such data. The statement must be renewed annually.

vi. Business Associate shall identify the security official who is responsible for the development and implementation of the policies and procedures required by 45 C.F.R. Part 164, Subpart C.

c. **Minimum Necessary.** With respect to any permitted Use, Disclosure, or request of PHI under this Agreement, Business Associate shall make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of such Use, Disclosure, or request respectively, as specified in 45 C.F.R. § 164.502(b).

d. **Business Associate's Agent.** Business Associate shall ensure that any agents, subcontractors, subawardees, vendors or others (collectively, "**Agents**") that Use or Disclose PHI and/or Confidential Information on behalf of Business Associate agree through a written agreement to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such PHI and/or Confidential Information.

8. **Mitigation of Harmful Effects.** Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI and other Confidential Information in violation of the requirements of this Agreement.

9. **Access to PHI.** Business Associate shall, to the extent Covered Entity determines that any PHI constitutes a Designated Record Set, make the PHI specified by Covered Entity available to the Individual(s) identified by Covered Entity as being entitled to access and copy that PHI. Business Associate shall provide such access for inspection of that PHI within fifteen (15) calendar days after receipt of request from Covered Entity. Business Associate shall also provide copies of that PHI ten (10) calendar days after receipt of request from Covered Entity. If Business Associate maintains an Electronic Health Record with PHI, and an Individual requests a copy of such information in electronic format, Business Associate shall make such information available in that format as required under the HITECH Act and 45 C.F.R. § 164.524.

10. **Amendment of PHI.** Business Associate shall, to the extent Covered Entity determines that any PHI constitutes a Designated Record Set, make PHI available for

amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. § 164.526 as requested by Covered Entity in the time and manner designated by Covered Entity.

11. **Accounting of Disclosures.** Business Associate shall document and make available to Covered Entity or (at the direction of Covered Entity) to an Individual, such disclosures of PHI and information related to such disclosures as necessary to respond to a proper request by the subject Individual for an accounting of disclosures of PHI in accordance with HIPAA, the HITECH Act and implementing regulations, including 45 C.F.R. § 164.528. Unless directed by Covered Entity to make available to an Individual, Business Associate shall provide to Covered Entity, within thirty (30) calendar days after receipt of request from Covered Entity, information collected in accordance with this Section 11 to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. Any accounting provided by Business Associate under this Section shall include:

a. The date of the disclosure;

b. The name, and address if known, of the entity or person who received the PHI;

c. A brief description of the PHI disclosed; and

d. A brief statement of the purpose of the disclosure.

For each Disclosure that could require an accounting under this Section, Business Associate shall document the information enumerated above, and shall securely maintain the information for six (6) years from the date of the Disclosure.

12. **Compliance with HITECH Act.** Business Associate shall comply with the requirements of Title XIII, Subtitle D, of the HITECH Act, which are applicable to business associates, and shall comply with the regulations promulgated thereunder.

13. **Compliance with Obligations of Covered Entity or DHCS.** To the extent Business Associate is to carry out an obligation of Covered Entity or DHCS under 45 C.F.R. Part 164, Subpart E, Business Associate shall comply with the requirements of such Subpart E that apply to Covered Entity or DHCS, as applicable, in the performance of such obligation.

14. **Access to Practices, Books and Records.** Business Associate shall make its internal practices, books, and records relating to the Use and Disclosure of PHI on behalf of Covered Entity available to Covered Entity upon reasonable request, and to the DHCS and the Secretary for purposes of determining Covered Entity's compliance with 45 C.F.R. Part 164, Subpart E. Business Associate also agrees to make its internal practices, books and records relating to the Use and Disclosure of PHI on behalf of Covered Entity available to DHCS, Covered Entity, and the Secretary for purposes of determining Business Associate's compliance with applicable requirements of HIPAA, the HITECH Act, CMIA, and implementing regulations. Business Associate shall immediately notify Covered Entity of any requests made by DHCS or the Secretary and provide Covered Entity with copies of any documents produced in response to such request.

15. **Return or Destroy PHI on Termination; Survival.** At termination of this Agreement, if feasible, Business Associate shall return to Covered Entity or, if agreed to by Covered Entity, destroy all PHI and other Confidential Information received from, or created or received by Business Associate on behalf of, Covered Entity that Business Associate or its Agents still maintains in any form, and shall retain no copies of such information. If Covered Entity elects destruction of PHI and/or other Confidential Information, Business Associate shall ensure such information is destroyed in accordance with the destruction methods specified in Sections 15(a) and 15(b) below, and shall certify in writing to Covered Entity that such information has been destroyed accordingly. If return or destruction is not feasible, Business Associate shall notify Covered Entity of the conditions that make the return or destruction infeasible. Subject to the approval of Covered Entity's regulator(s) if necessary, if such return or destruction is not feasible, Covered Entity shall determine the terms and conditions under which Business Associate may retain the PHI. Business Associate shall also extend the protections of this Agreement to the information and limit further Uses and Disclosures to those purposes that make the return or destruction of the information infeasible.

a. **Data Destruction.** Data destruction methods for Covered Entity PHI or Confidential Information must conform to the NIST Special Publication 800-88. Other methods require prior written permission of Covered Entity and, if necessary, Covered Entity's regulator(s).

b. **Destruction of Hard Copy Confidential Data.** Covered Entity PHI or Confidential Information in hard copy form must be disposed of through confidential means, such as crosscut shredding and pulverizing.

16. **Special Provision for SSA Data.** If Business Associate receives data from or on behalf of Covered Entity that was verified by or provided by the Social Security Administration ("**SSA Data**") and is subject to an agreement between DHCS and SSA, Business Associate shall provide, upon request by Covered Entity, a list of all employees and Agents and employees who have access to such SSA Data, including employees and Agents of its Agents, to Covered Entity.

17. **Breaches and Security Incidents.** Business Associate shall implement reasonable systems for the discovery and prompt reporting of any Breach or Security Incident, and take the following steps:

a. **Notice to Covered Entity.**

i. **Immediate Notice.** Business Associate shall notify Covered Entity immediately upon the discovery of a suspected Breach or Security Incident that involves SSA Data. This notification will be provided by email upon discovery of the Breach. If Business Associate is unable to provide notification by email, then Business Associate shall provide notice by telephone to Covered Entity.

ii. **24-Hour Notice.** Business Associate shall notify Covered Entity within twenty-four (24) hours by email (or by telephone if Business Associate is unable to email Covered Entity) of the discovery of the following, unless attributable to treatment provider that is not acting as a business associate of Business Associate:

1. Unsecured PHI if the PHI is reasonably believed to have been accessed or acquired by an unauthorized person;

2. Any suspected Security Incident which risks unauthorized access to PHI and/or other Confidential Information;

3. Any intrusion or unauthorized access, Use or Disclosure of PHI in violation of this Agreement; or

4. Potential loss of confidential data affecting this Agreement.

iii. Notice shall be provided to the Covered Entity Privacy Officer ("**Covered Entity Contact**") using the Covered Entity Contact Information at Section 17(g) below. Such notification by Business Associate shall comply with Covered Entity's form and content requirements for reporting privacy incident and shall include all information known at the time the incident is reported.

b. **Required Actions.** Upon discovery of a Breach or suspected Security Incident, intrusion or unauthorized access, use or disclosure of PHI, Business Associate shall take:

i. Prompt action to mitigate any risks or damages involved with the Security Incident or Breach;

ii. Any action pertaining to such unauthorized disclosure required by applicable federal and state law; and

iii. Any corrective actions required by Covered Entity or Covered Entity's regulator(s).

c. **Investigation.** Business Associate shall immediately investigate such Security Incident or confidential Breach. Business Associate shall comply with Covered Entity's additional form and content requirements for reporting such privacy incident.

i. Incident details including the date of the incident and when it was discovered;

ii. The identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been accessed, acquired, used or disclosed during the Breach;

iii. The nature of the data elements involved and the extent of the data involved in the Breach;

iv. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data;

v. A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized;

vi. A description of the probable causes of the improper Use or Disclosure;

vii. Any other available information that the Business Associate is required to include in notification to the Individual under 45 C.F.R. § 164.404(c);

viii. Whether the PHI or confidential data that is the subject of the Security Incident, Breach, or unauthorized Use or Disclosure of PHI or confidential data included Unsecured PHI;

ix. Whether a law enforcement official has requested a delay in notification of Individuals of the Security Incident, Breach, or unauthorized Use or Disclosure of PHI or Confidential Information because such notification would impede a criminal investigation or damage national security and whether such notice is in writing; and

x. Whether Section 13402 of the HITECH Act (codified at 42 U.S.C. § 17932), California Civil Code §§ 1798.29 or 1798.82, or any other federal or state laws requiring individual notifications of breaches are triggered.

d. **Complete Report.** Business Associate shall provide a complete written report of the investigation ("**Final Report**") to the Covered Entity Contact within seven (7) working days of the discovery of the Security Incident or Breach. Business Associate shall comply with Covered Entity's additional form and content requirements for reporting of such privacy incident.

i. The Final Report shall provide a comprehensive discussion of the matters identified in Section 17(c), above and the following:

1. An assessment of all known factors relevant to a determination of whether a Breach occurred under HIPAA and other applicable federal and state laws;

2. A full, detailed corrective action plan describing how Business Associate will prevent reoccurrence of the incident in the future, including its implementation date and information on mitigation measures taken to halt and/or contain the improper Use or Disclosure and to reduce the harmful effects of the Breach. All corrective actions are subject to the approval of Covered Entity and Covered Entity's regulator(s), as applicable; and

3. The potential impacts of the incident, such as potential misuse of data and identity theft.

ii. If Covered Entity or Covered Entity's regulator(s) requests additional information, Business Associate shall make reasonable efforts to provide Covered Entity with such information. A supplemental written report may be used to submit revised or additional information after the Final Report is submitted.

iii. Covered Entity and Covered Entity's regulator(s), as applicable, will review and approve or disapprove Business Associate's determination of whether a Breach occurred, whether the Security Incident or Breach is reportable to the appropriate entities, if individual notifications are required, and Business Associate's corrective action plan.

iv. **New Submission Timeframe.** If Business Associate does not complete a Final Report within the seven (7) working day timeframe specified in Section 17(d) above, Business Associate shall request approval from Covered Entity within the seven (7) working day timeframe of a new submission timeframe for the Final Report. Business Associate acknowledges that a new submission timeframe requires the approval of Covered Entity and, if necessary, Covered Entity's regulator(s).

e. **Notification of Individuals.** If the cause of a Breach is attributable to Business Associate or its Agents, other than when attributable to a treatment provider that is not acting as a business associate of Business Associate, Business Associate shall notify Individuals accordingly and pay all costs of such notifications, as well as costs associated with the Breach. The notifications shall comply with applicable federal and state law. All such notifications shall be coordinated with Covered Entity. Covered Entity and Covered Entity regulator(s), as applicable, shall approve the time, manner and content of any such notifications. Business Associate acknowledges that such review and approval by Covered Entity and Covered Entity regulator(s), as applicable, must be obtained before the notifications are made.

f. **Responsibility for Reporting of Breaches to Entities Other than Covered Entity.** If the cause of a Breach of PHI is attributable to Business Associate or Agents, other than when attributable to a treatment provider that is not acting as a business associate of Business Associate, Business Associate agrees that Covered Entity shall make all required reporting of the Breach as required by applicable federal and state law, including any required notifications to media outlets, the Secretary, and other government agency/regulator.

g. **Covered Entity Contact Information.** To direct communications to Covered Entity Privacy Officer, the Business Associate shall initiate contact as indicated here. Covered Entity reserves the right to make changes to the contact information below by giving written notice to Business Associate. These changes shall not require an amendment to this Agreement.

If to MCP's Privacy Officer:

Privacy Officer
c/o: Office of Compliance
CalOptima
505 City Parkway West
Orange, CA 92868

Email: privacy@caloptima.org

Telephone: (714) 246-8400 (ask the operator to connect to Privacy Officer)

If to County Privacy Officer:

Kelly K. Sabet, LCSW, CHC, CHPC
Chief Compliance Officer
405 W. 5th St, #212

Santa Ana, CA 92701

Email: officeofcompliance@ochca.com

Telephone: (714) 581-7769

18. **Responsibilities of Covered Entity.**

a. Covered Entity agrees to not request the Business Associate to Use or Disclose PHI in any manner that would not be permissible under HIPAA and/or other applicable federal and/or state law.

b. **Notification of SSA Data.** Covered Entity shall notify Business Associate if Business Associate receives data that is SSA Data from or on behalf of Covered Entity.

19. **Indemnification.** Business Associate will immediately indemnify and pay Covered Entity for and hold it harmless from (i) any and all fees and expenses Covered Entity incurs in investigating, responding to, and/or mitigating a Breach of PHI or Confidential Information caused by Business Associate or its Agents; (ii) any damages, attorneys' fees, costs, liabilities or other sums actually incurred by Covered Entity due to a claim, lawsuit, or demand by a third party arising out of a Breach of PHI or Confidential Information caused by Business Associate or its Agents; and/or (iii) for fines, assessments and/or civil penalties assessed or imposed against Covered Entity by any government agency/regulator based on a Breach of PHI or Confidential Information caused by Business Associate or its Agents. Such fees and expenses may include, without limitation, attorneys' fees and costs and costs for computer security consultants, credit reporting agency services, postal or other delivery charges, notifications of Breach to Individuals and regulators, and required reporting of Breach. Acceptance by Covered Entity of any insurance certificates and endorsements required under the MOU does not relieve Business Associate from liability under this indemnification provision. This provision shall apply to any damages or claims for damages whether or not such insurance policies shall have been determined to apply.

20. **Audits, Inspection and Enforcement.**

a. From time to time, Covered Entity and/or Covered Entity's regulator(s) may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Agreement. Business Associate shall promptly remedy any violation of this Agreement and shall certify the same to the Covered Entity Privacy Officer in writing. Whether or how Covered Entity or Covered Entity's regulator(s) exercises this provision shall not in any respect relieve Business Associate of its responsibility to comply with this Agreement.

b. If Business Associate is the subject of an audit, compliance review, investigation or any proceeding that is related to the performance of its obligations pursuant to this Agreement, or is the subject of any judicial or administrative proceeding alleging a violation of HIPAA, Business Associate shall promptly notify Covered Entity unless it is legally prohibited from doing so.

21. **Term and Termination.**

a. **Term.** This Exhibit A is effective as of the Effective Date and shall terminate (i) when the MOU terminates, (ii) in accordance with this Section 21, or (iii) when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in Section 15.

b. **Termination for Cause.** Upon Covered Entity's knowledge of a violation of this Agreement by Business Associate, Covered Entity may in its discretion:

i. Provide an opportunity for Business Associate to cure the violation and terminate this Agreement if Business Associate does not do so within the time specified by Covered Entity; or

ii. Terminate this Agreement if Business Associate has violated a material term of this Agreement.

iii. **Judicial or Administrative Proceedings.** Covered Entity may terminate this Agreement if Business Associate is found to have violated HIPAA, or stipulates or consents to any such conclusion, in any judicial or administrative proceeding.

22. **Miscellaneous Provisions.**

a. **Disclaimer.** Covered Entity makes no warranty or representation that compliance by Business Associate with this Agreement will satisfy Business Associate's business needs or compliance obligations. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI and other Confidential Information.

b. **Amendment.**

i. Any provision of this Agreement which is in conflict with current or future applicable federal or state laws is hereby amended to conform to the provisions of those laws. Such amendment of this Agreement shall be effective on the effective date of the laws necessitating it, and shall be binding on the Parties even though such amendment may not have been reduced to writing and formally agreed upon and executed by the Parties.

ii. This Agreement shall be deemed amended to comply with future changes in applicable laws or regulations (a "**Regulatory Change**") as of the date a Regulatory Change goes into effect, even if the Regulatory Change is not reduced to writing and formally agreed upon by the Parties.

iii. Failure by Business Associate to take necessary actions required by amendments to this Agreement under Section 22(b)(i) or 22(b)(ii) shall constitute a material violation of this Agreement.

c. **Assistance in Litigation or Administrative Proceedings.** Business Associate shall make itself and its employees and Agents available to Covered Entity or Covered Entity's regulator(s) at no cost to Covered Entity or Covered Entity's regulator(s), as applicable, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against Covered Entity or Covered Entity's regulator(s), their respective directors, officers and/or employees based upon claimed violation of HIPAA, which involve inactions or actions by the Business Associate.

d. **No Third-Party Beneficiaries.** Nothing in this Agreement is intended to or shall confer, upon any third person any rights or remedies whatsoever.

e. **Interpretation.** The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA and other applicable laws.

f. **No Waiver of Obligations.** No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

g. **Statutory or Regulatory Reference.** Any reference to statutory or regulatory language in this Agreement shall be to such language as in effect or as amended.

h. **Injunctive Relief.** Notwithstanding any rights or remedies provided in this Agreement, Covered Entity retains all rights to seek injunctive relief to prevent or stop the unauthorized Use or Disclosure of PHI or Confidential Information by Business Associate or any agent, subcontractor, employee or third party that received PHI or Confidential Information, and Business Associate agrees that Covered Entity may seek injunctive relief under this section without any requirement to prove actual monetary damage or post a bond or other security.

i. **Monitoring.** As applicable, Business Associate shall comply with monitoring requirements of Covered Entity's contracts with regulator(s) or any other monitoring requests by Covered Entity's regulator(s).