Exhibit A
Scope of Work

1. Service Overview

This section provides an overview of the Children and Youth Behavioral Health Initiative (CYBHI) and the statewide, multi-payer, school-linked fee schedule (CYBHI Fee Schedule) and school-linked behavioral health provider network (provider network). Carelon Behavioral Health, Inc. (Contractor) agrees to meet or exceed the requirements, described herein and specified throughout the entirety of this Contract between the Contractor and the California Department of Health Care Services (DHCS).

A. Background on Children and Youth Behavioral Health Initiative (CYBHI)

As a key feature of Governor Newsom's Master Plan for Kids' Mental Health[1], the CYBHI is a multiyear, multi-department package of investments that reimagines the systems that support behavioral health for all California's children, youth, and their families, regardless of payer. Efforts focus on promoting social and emotional well-being, preventing behavioral health challenges, and providing equitable, appropriate, timely, and accessible services for emerging and existing behavioral health needs for children and youth ages 0-25, with the following goals[2]:

1) Advance Equity: All children, youth and their families have access to linguistically, culturally, and developmentally appropriate services and supports.

2) Designed for Youth by Youth: Children and youth are engaged in the design and implementation of services and supports; ensuring that programs center on their needs.

3) Start Early, Start Smart: The systems that support children, youth and their families act early by promoting positive mental health and reducing risk for more significant mental health needs and challenges.

4) Center around Children and Youth: Across all levels of government, child- and youth-serving agencies form coordinated systems of care to deliver high- quality behavioral health programs responsive to the needs of children and youth and their families.

5) Empower Families and Communities: People who teach, work with or care for children and youth are equipped to recognize signs of poor mental health or substance use and know how to access supports.

6) Right Time, Right Place: Youth and children can access high-quality care and information when they need it — including early mornings, evenings,

[1] Governor Newsom's Master Plan for Kids' Mental Health (Link)
[2] Children and Youth Behavioral Health Initiative Brief (Link)

and weekends and where they need it — including where they live, learn, and play.

7) Free of Stigma: Children youth and their families can talk about their mental health and well-being and seek help without feeling ashamed or fearing discrimination.

B. CYBHI Fee Schedule Overview

As part of the CYBHI, the State of California will increase access to behavioral health services. The DHCS, in collaboration with the Department of Managed Health Care (DMHC) and the California Department of Insurance (CDI), will establish the CYBHI Fee Schedule for a set of outpatient mental health and substance use disorder (SUD) services provided to a student 25 years of age or younger at a school or school-linked site[3].

The CYBHI Fee Schedule will establish a permanent, sustainable reimbursement mechanism for school-linked behavioral health services that:

1) Increases access to school-linked behavioral health services for children and youth;

2) Applies to multiple payers, including Medi-Cal Managed Care Plans, commercial health plans, and disability insurers (collectively, MCPs);

3) Expands the types of practitioners eligible for reimbursement for school-based behavioral health services to include Pupil Personnel Services (PPS) credentialed providers[4] and Wellness Coaches[5];

4) Creates a more approachable reimbursement model for schools, given the shift to fee-for-service reimbursement (as opposed to existing cost resettlement programs);

5) Eases burdens around contracting, rate negotiation and navigation of delivery systems with State-established rates for all included services; and,

6) Provides state-funded supports for payers and providers, with a third-party administrator being piloted in 2024 to manage the provider network and facilitate claims administration/payment remittance.

C. School-linked behavioral health provider network overview

[3] California Welfare and Institutions (W&I) Code Section 5971.4 (Link)
[4] Inclusion of Pupil Personnel Services credentialed providers is pending State Plan Amendment approval from CMS
[5] Inclusion of Wellness Coaches will go live in 2025

Exhibit A
Scope of Work

The CYBHI statute requires DHCS to develop and maintain a school-linked statewide provider network of school site behavioral health counselors.[6] Only those county offices of education (COE), local education agencies (LEAs), institutions of higher education (IHE), providers and practitioners identified as part of this network will be eligible for reimbursement under the CYBHI Fee Schedule. LEAs and IHEs that are approved to participate in the provider network will be responsible for:

1) Enrolling in the Medi-Cal program as a provider;
2) Signing an LEA or IHE provider participation agreement;
3) Executing applicable data-sharing agreements;
4) Submitting and maintaining a designated (i.e., eligible) provider list including all employed or affiliated practitioners and providers;
5) Providing or arranging for the provision of covered services to students under the age of 26;
6) Preparing claims with the support of a third-party administrator (TPA);
7) Receiving and disseminating payments, as applicable; and,
8) Reporting data to DHCS and Contractor.

2. Service Location and Hours

The CYBHI services will be performed at various locations in the State of California as specified by DHCS. The services must be provided Monday through Friday during normal business hours, excluding official holidays.

3. Contract Period

This Contract will be effective from January 1, 2024 – July 30, 2027. At any time prior to the expiration of the Contract, the parties may, by mutual written agreement, extend the Contract under the terms of this Agreement for such additional periods as they may agree.

[6] W&I Code § 5961(b)

Exhibit A
Scope of Work

4. Project Representatives

A. The project representatives during the term of this Agreement will be:

Department of Health Care Services	Carelon Behavioral Health , Inc.
Contract Manager: Kenna Cook Telephone: (916) 313-7010 Email: kenna.cook@dhcs.ca.gov	Contract Manager: Christina Kim Telephone: (562) 545-1741 Email: christina.kim@carelon.com

B. Direct all inquiries to:

Department of Health Care Services	Carelon Behavioral Health, Inc.
Office of Strategic Partnerships Attention: Kenna Cook 1501 Capitol Avenue Sacramento, CA 95814 Telephone: (916) 313-7010 Email: kenna.cook@dhcs.ca.gov	Attention: Christina Kim Carelon Behavioral Health 200 State Street, 3rd Floor Boston, MA 02109 Telephone: (562) 545-1741 Email: christina.kim@carelon.con

C. Either party may make changes to the information above by giving written notice to the other party. Said changes will not require an amendment to this Agreement.

5. Services to be Performed

A. Provider network management

1) Contractor will manage and oversee a school-linked, behavioral health provider network comprised of LEAs, public IHEs, and their designated providers and practitioners in accordance with DHCS guidance.

2) As a prerequisite for participation in this network, LEAs and IHEs must be enrolled into the Medi-Cal program. Approved LEAs and IHEs will be identified in DHCS Provider Master File. Contractor must confirm the Medi-Cal enrollment of the LEA or IHE prior to processing network credentialing applications or claims for payment.

3) Designated Provider List

a. Contractor will develop and implement processes to intake listings of designated providers and practitioner from all enrolled and participating LEAs and IHEs. The lists will specify all behavioral health providers and practitioners employed or contracted/affiliated with the LEAs or IHEs and deemed eligible by the LEA or IHE to

Exhibit A
Scope of Work

participate in the CYBHI Fee Schedule program, and must identify all eligible employed, contracted, and affiliated individual practitioners or organizational providers.

b. LEAs and IHEs must submit, at minimum, monthly updates to the designated provider list.

c. Contractor will prepare and submit to DHCS, on a monthly basis, a compiled designated provider list (e.g., roster) of all providers deemed eligible for submitting claims as part of the CYBHI Fee Schedule program. The compiled provider list will be public-facing and posted on the DHCS website.

    i. Contractor must remediate all public-facing documents to ensure postings meet requirements of the Americans with Disabilities Act and any other applicable state or federal laws.

    ii. Contractor will use DHCS-approved branding assets and design elements, including color, schema, logo, typography, graphic elements, etc. in all public-facing postings.

d. No later than thirty (30) calendar days after execution of this Contract, Contractor must submit to DHCS, for approval, a policy and procedure for the designated provider list, including proposed data elements, data collection methods, processes for verifying eligibility and communicating approvals to participating LEAs and IHEs. This procedure must also address processes for compiling the provider list. DHCS may publish a provider list on its web site.

e. Upon approval, Contractor may request modifications to the proposed structure of the designated provider list or associated procedures by submitting such a request to DHCS in writing.

f. DHCS may request Contractor to make modifications with advance notice of a minimum of fourteen (14) business days.

g. Contractor must implement requested modifications within fourteen (14) business days of receiving such a request from DHCS.

Exhibit A
Scope of Work

4) Screening, Credentialing and Re-Credentialing

a. Contractor will conduct provider screening, credentialing and re-credentialing activities for all participating entities, including the LEAs, IHEs and any designated providers identified by LEAs or IHEs, as required for the particular provider type.

b. For the purposes of the CYBHI Fee Schedule, DHCS expects MCPs to delegate screening and enrollment activities to Contractor.

c. Contractor must verify the Medi-Cal provider enrollment status for any individual practitioners or organizational providers identified by the LEA or IHE.

d. Contractor must verify the identity and determine the exclusion and/or enrollment status of all providers and practitioners by checking all of the following databases, as applicable:

    i. Social Security Administration's Death Master File;

    ii. National Plan and Provider Enumeration System (NPPES);

    iii. List of Excluded Individuals/Entities (LEIE);

    iv. System for Award Management (SAM);

    v. Centers for Medicare & Medicaid Services' (CMS) Medicare Exclusion Database (MED);

    vi. DHCS' Suspended and Ineligible Provider List;

    vii. Restricted Provider Database (RPD); and,

    viii. CalHHS Open Data Portal.

e. In addition to checking all the databases upon a provider's enrollment/reenrollment, Contractor must also review the SAM and LEIE databases on a regular basis, and at least monthly, to ensure that participating and designated providers continue to meet enrollment criteria. Contractor must implement processes to notify DHCS, LEAs or IHEs in connection with any identified excluded providers. Each participating provider must maintain good standing in the Medicare and Medicaid/Medi-Cal programs. Any provider terminated from the Medicare or Medicaid/Medi-Cal program may not participate in the CYBHI Fee Schedule network.

Exhibit A
Scope of Work

f. Contractor must verify the credentials of designated practitioners and providers, as required for the particular provider type, through a primary source, as applicable, including verifying the following:

   ix. The appropriate license, credential, board certification or registration.

   x. Evidence of graduation or completion of any required education.

   xi. Proof of completion of any relevant medical residency and/or specialty training, as applicable.

   xii. Additional information that the Contractor will receive and verify include the following (as applicable):

      1. Work history;

      2. Hospital and clinic privileges in good standing;

      3. History of any suspension or curtailment of hospital and clinic privileges;

      4. Current Drug Enforcement Administration identification number;

      5. National Provider Identifier number;

      6. Current malpractice insurance in an adequate amount, as required for the particular provider type;

      7. History of liability claims against the provider;

      8. Provider information, if any, entered in the National Practitioner Data Bank, when applicable; and,

      9. History of sanctions from participating in Medicare and/or Medicaid/Medi-Cal.

g. No later than sixty (60) calendar days after execution of this Contract, Contractor must develop and submit to DHCS, for approval, its policy and procedures detailing credentialing activities and steps Contractor will take to verify Medi-Cal eligibility, licensure or credential status, and other requirements specified in DHCS All-Plan Letter 22-013, or subsequently published superseding guidance. Contractor's policy and procedure must also address timelines for conducting screening and credentialing activities and processes for reporting results of screening,

Exhibit A
Scope of Work

credentialing and re-credentialing activities to MCPs, LEAs, IHEs, and DHCS (when applicable).

h. Once approved, Contractor may request modifications to its policy and procedure by submitting to DHCS the requested modifications along with the justification for the change. Contractor must submit such change requests no later than fourteen (14) calendar days prior to effectuating any changes to its policy and procedure.

i. DHCS may request Contractor to make California specific modifications in compliance with state guidance with advance notice of a minimum of fourteen (14) business days.

j. Where technically and operationally feasible, Contractor must implement requested modifications within fourteen (14) business days of receiving such a request from DHCS. If technological or operational work is necessary to implement proposed modifications, Contractor may propose to DHCS, for approval, an alternate timeframe for implementation.

B. Claims Administration and Payment Remittance

1) Contractor will serve as the single, centralized statewide claims clearinghouse for the CYBHI Fee Schedule program.

2) Contractor will manage the claims platform and process fee schedule claims, in accordance with this Contract, as follows:

a. Contractor will establish the technical infrastructure for processing claims submitted by LEAs, IHEs, and designated providers.

b. Contractor will define the dataset required for claims in accordance with federal and state standards and requirements.

c. Contractor will process all claims information from designated providers/practitioners for services furnished to students in a school-linked setting.

d. Contractor will submit clean claims for payment to the applicable MCP.

e. Contractor will establish the technical infrastructure for payment remittance, including receiving payments from the MCPs and transferring such payments to the LEAs, IHEs, and/or designated providers or practitioners.

f. Contractor must not retain any portion of payments received from MCPs and shall remit all MCP payments to the applicable LEAs, IHEs, and/or designated providers or practitioners.

Exhibit A
Scope of Work

3) Claims Validation

a. Contractor will review the claim upon receipt and determine eligibility for payment under the fee schedule based upon DHCS business rules, which will include, but not be limited to, verification of the following:

i. Data validity: All required data elements are contained in the submitted claim and include valid data inputs;

ii. Procedure compatibility: The service provided on the claim is a qualifying code and able to be rendered under the fee schedule;

iii. The appropriate payment rate as established in the fee schedule;

iv. Provider eligibility on the date of service: The provider is a part of the provider network;

v. Designated provider/practitioner eligibility on the date of service: The rendering provider/practitioner is eligible to render the fee schedule service specified in the claim and possesses the necessary credentials and licensures to administer the service;

vi. CYBHI recipient eligibility is the responsibility of the LEA on the date of service: The student receiving the services is an eligible individual under the fee schedule guidelines (e.g., under 26 years of age, listed on the student roster provided by the LEA or public institution of higher education); and,

vii. Claim duplication: The service submitted is non-duplicative with other claims submitted to Contractor for payment.

b. While Contractor will make best efforts to validate the above information based on information known at the time of processing, Contractor may reasonably rely on information provided by the MCPs and the LEAs, IHEs, and other designated providers, and shall not bear any liability for any issues later identified that are the result of information submitted to Contractor that was not accurate or up-to-date, or related to any retroactive eligibility or other determinations.

4) Coordination of Benefits

Exhibit A
Scope of Work

a. Contractor will coordinate benefits for students by matching enrollee data (i.e., student information) to the applicable MCP payer responsible for coverage.

b. Contractor will establish processes to intake student information and enrollee data to facilitate benefits coordination.

c. Contractor will create a comprehensive student (member) roster based on student information submitted by LEAs, public IHEs, and/or the MCPs or disability insurers. Contractor may rely on information received by LEAs or public IHEs and is only responsible for coordinating benefits based on information received by LEAs/public IHEs, and as allowed by FERPA.

d. No later than thirty (30) calendar days after Contract execution, Contractor must submit to DHCS, for approval, its policy and procedure for benefits coordination, including the proposed structure and relevant data fields for the student information/member roster. This information will be collected by LEAs and IHEs and submitted to the Contractor at a frequency established by Contractor, as detailed in the policy. Information will include, but not be limited to the following:

    i. Student name

    ii. Student date of birth

    iii. Payer name

    iv. Insurance ID number

    v. Group number

    vi. Other fields, as applicable

e. Once approved, Contractor may request modifications to its policy and procedure by submitting to DHCS the requested modifications along with the justification for the change. Contractor must submit such change requests no later than fourteen (14) calendar days prior to effectuating any changes to its policy and procedure.

f. DHCS may request Contractor to make modifications with advance notice of a minimum of fourteen (14) business days.

g. Where technically and operationally feasible, Contractor must implement requested modifications within fourteen (14) business days of receiving such a request from DHCS. If technological or operational work is necessary to implement proposed modifications,

Exhibit A
Scope of Work

Contractor may propose to DHCS, for approval, an alternate timeframe for implementation. If modifications are infeasible, failure to complete modifications may be cause for termination of the Contract.

h. If the individual is eligible for healthcare benefits through insurers other than those included under CYBHI Statewide Fee Schedule requirements (e.g., ERISA plans; uninsured individuals; out of state commercial insurers; other non-Medi-Cal government programs; etc.), the Contractor will reject the claim and issue the provider an explanation that the claim must be sent to the appropriate payer for potential coverage.

i. Contractor will develop and submit its policies and procedures, for DHCS approval, pertaining to claims denials, payments, overpayments and recoupment in cases where the claim is deemed ineligible for reimbursement because of insurance coverage status, changes in payer responsibility to pay, or other related denials.

5) Claims Submission

a. Contractor will ensure a clean claim[7] is prepared for submission to the applicable MCP payer within the timeframes identified within the Contractor's policies and procedures, as approved by DHCS, by verifying the submitted claim has been prepared in accordance with standards as defined by DHCS (e.g., National Uniform Billing Committee or National Uniform Claim Committee standards), which must include, but will not be limited to, the following information:

i. Description of the service rendered using valid Current Procedural Terminology (CPT) codes, along with the number of days or units for each service;

ii. Member (patient) demographic information which must include at minimum the individual's last name, first name, and date of birth;

iii. Provider Information, including name, address, National Provider Identifier (NPI), tax identification number (TIN) (the information submitted by the provider must match the format that is in the provider master file / maintained as the provider network directory by the Contractor), and the

[7] A "clean claim" is defined in Title 42 of the Code of Federal Regulations (CFR), Section 447.45(b). Clean claim means "one that can be processed without obtaining additional information from the provider of the service or from a third party. It includes a claim with errors originating in a State's claims system. It does not include a claim from a provider who is under investigation for fraud or abuse, or a claim under review for medical necessity." (Link)

Exhibit A
Scope of Work

provider type / any additional modifiers needed to distinguish providers rendering fee schedule services;

iv. CYBHI Code, which establishes the claim as being submitted under the fee schedule;

v. Valid date(s) of service;

vi. Billed amount; and,

vii. Date and signature of person submitting claim or name of designated provider/practitioner who rendered service(s).

b. Contractor will confirm the submitted claim is complete and accurate in accordance with the relevant DHCS, DMHC, and California Department of Insurance (CDI) standards and accept or reject the submitted claim.

c. Contractor will return rejected claims to the submitter with supporting explanation and opportunity for resubmission upon correction.

d. If the individual is eligible for healthcare benefits through insurers other than those included under CYBHI Statewide Fee Schedule requirements (e.g., ERISA plans; uninsured individuals; out of state commercial health plans; other non-Medi-Cal government programs; etc.), the Contractor will reject the claim and send back to provider with an explanation that the claim must be sent to the appropriate payer for potential coverage.

e. Contractor will maintain a tracking system for each submitted claim, which will include the status of claims through each step of the claims processing, as appropriate, which includes, but is not limited to, the following:

i. Claims entry;

ii. Claims adjudication;

iii. Claims payment;

iv. Claims reporting;

v. Claims denials and appeals; and,

vi. Other claims statuses, as applicable

Exhibit A
Scope of Work

f. Contractor will provide the necessary access for MCPs, LEAs, IHEs and designated providers and practitioners to view the status of any claim for services they have delivered at any given point.

6) Payment Remittance

a. Contractor is responsible for claims reconciliation and payment. Under no circumstance shall Contractor be responsible for funding claims. Timely payment requirements shall begin when the clean claim is submitted by Contractor to the MCO on behalf of the provider. Contractor will monitor and verify whether the payer of responsibility distributes the payments of claims in accordance with the published CYBHI Fee Schedule and in accordance with the established timelines for each payer upon receiving a clean claim or accepted encounter for qualifying services as referenced in the table below:

Department	**Timely payment requirement**	**Source**
DHCS	No later than 30 calendar days after claim receipt for 90% of all clean claims[8] In addition, 99% of all clean claims[8] will be paid within ninety (90) days of receipt	APL 23-020, 42 CFR 447.45 and 447.46
DMHC	No later than 30 working days after claim receipt (45 working days for HMOs)	CA Health & Safety Code Section 1371
CDI	No later than 30 working days after claim receipt	CA Insurance Code Sections 10123.13 and 10123.147
Specialized Plans Contracting with HMO	Deliver, furnish or otherwise arrange for services for that plan's enrollees and must reimburse complete claims received for those services within 30 working days.	28 CCR 1300.71(g)(4)

b. In accordance with timely payment requirements above, Contractor will execute an electronic payment transaction to ensure the appropriate LEA provider or practitioner receives the reimbursement payment for rendered services.

Exhibit A
Scope of Work

c. Contractor will ensure LEAs, IHEs, and/or designated providers or practitioners have the capability to submit adjustments or voids on previously adjudicated claims, including those processed within the same pay cycle, using the edit and pricing rules applicable to the original claim's dates of service and associate them with the original claim.

d. Contractor must, on a monthly basis, submit a report to DHCS identifying payment status, including late payments not paid accordance with established timelines. Contractor shall facilitate billing and reimbursement practice education and outreach to the LEAs and MCPs.

e. Contractor will coordinate third-party liability (TPL)/benefits and shall ensure all billable services are submitted to Medi-Cal and other third-party payers, and that Medi-Cal Fee-for-Service (FFS) is used to reimburse providers for statewide fee schedule services as the payer of last resort. Contractor shall submit claims to MCPs, FFS Medi-Cal, and other third-party payers using the required procedure code billing.

f. Contractor will continue to monitor billings until payment is received and deemed valid.

g. Contractor shall ensure all payments to LEA and/or IHE service providers are made in accordance with the established reimbursement methodology using the CYBHI statewide fee schedule.

h. Contractor shall receive payment from the MCP and pay the claim in compliance with the timely claims' payment requirements outlined in table 6a. In no event shall the Contractor be responsible for funding claims that MCP or other responsible party has failed to fund.

i. Contractor shall ensure claims are paid or denied within a timely manner from the date of receipt of such claims. Notwithstanding the above, Contractor shall not be bound by the referenced claim's timely payment requirements or held liable due to the failure of the MCP to adjudicate and pay claims within such timely payment requirements. Contractor is not financially responsible for MCP non-payments.

j. Claims deemed to be appropriate and meeting the requirements of the CYBHI program that remain unpaid for 45 days by MCPs will be reported to DHCS and DMHC or CDI, as applicable.

Exhibit A
Scope of Work

k. In the event of a claim denial, the Contractor shall notify LEAs or IHEs of any decision to deny a claim. Notifications shall include the reason the denying entity provided Contractor for the denial, and the contact information for the submission of claims. This information shall also be provided if the denying entity is a subcontractor or MCP. LEA and IHE providers and practitioners will be provided with appeal procedures including those outlined by DHCS and the CBYHI program.

7) No later than thirty (30) calendar days after execution of this Contract, Contractor must submit to DHCS, for approval, a proposed claims workflow plan, including the end-to-end processes from claims intake to payment remittance. The Claims Workflow Plan must, at a minimum, address the following: claims preparation, claims review, intake and verification of student insurance coverage and coordination of benefits, verification of provider eligibility, claims submission, claims processing timelines, payment remittance, appeals and denials procedures, overpayment recovery procedures, storage and maintenance of claims records, and reporting processes.

8) Once approved, Contractor may request modifications to its policy and procedure by submitting to DHCS the requested modifications along with the justification for the change. Contractor must submit such change requests no later than fourteen (14) calendar days prior to effectuating any changes to its policy and procedure.

9) DHCS may request Contractor to make modifications with advance notice of a minimum of fourteen (14) business days.

10) Where technically and operationally feasible, Contractor must implement requested modifications within fourteen (14) business days of receiving such a request from DHCS. Should technological or operational work be necessitated to implement proposed modifications, Contractor to engage in discussion with DHCS regarding a reasonable timeframe for implementation.

C. Quality Monitoring and Provider Network Oversight

1) Contractor will conduct ongoing quality monitoring and oversight activities for each participating LEA, IHE, and designated providers. Contractor will monitor the network of designated providers/practitioners, including performance monitoring and upholding of quality standards that are consistent with broader Medi-Cal, commercial health plans, and disability insurers' requirements and any additional quality standards as outlined by DHCS as part of the CYBHI.

Exhibit A
Scope of Work

2) Upon enrollment of designated providers/practitioners in the provider network, Contractor will monitor ongoing compliance, including timely revalidation, recertification, and recredentialing as required, ongoing review of screening, credentialing, and other eligibility data, and monitoring for potentially adverse information such as sanctions, exclusions, license expirations, fraud allegations, and criminal convictions.

3) On a monthly basis, Contractor will query the relevant set of databases used to verify eligibility of designated providers/practitioners to ensure that enrolled providers continue to meet eligibility criteria.

4) Contractor will take appropriate action based on any findings during the monthly monitoring process (e.g., remediation, corrective actions, removal from participation in the provider network), as each designated provider/practitioner enrolled in the provider network must maintain good standing in the Medicare and Medicaid/Medi-Cal programs.

5) Contractor will notify DHCS and the providers or practitioners within thirty (30) calendar days of discovery if any designated providers or practitioners submitted for participation in the provider network are at any point flagged to require additional screening, revalidation, or termination/suspension from participation in the provider network and will maintain records of all status changes throughout the duration of this contract.

6) Contractor will establish processes and technical safeguards to prevent the processing of claims submitted by ineligible providers/practitioners.

7) Contractor will be required to retain all provider and practitioner screening and enrollment materials and documents for ten years. Additionally, the Contractor must make all screening and enrollment documents and materials available to DHCS, CMS, and any other authorized governmental entities upon request in a timeframe determined to be reasonable based on the amount and scope of information requested.

8) Contractor will establish processes for timely review, adjudication, and resolution of member and provider grievances including with respect to coordination with MCPs regarding the same.

9) No later than forty-five (45) calendar days after execution of this Contract, Contactor must submit to DHCS, for approval, a monitoring and quality oversight plan detailing its policies and procedures for conducting quality oversight and monitoring of the provider network and claims to ensure program integrity. The plan will also address Contractor’s proposed

Exhibit A
Scope of Work

approach for conducting quality oversight of services rendered to students by designated providers and practitioners (including LEAs and IHEs), including its processes for adjudicating grievances.

10) Once approved, Contractor may request modifications to its policy and procedure by submitting to DHCS the requested modifications along with the justification for the change. Contractor must submit such change requests no later than fourteen (14) calendar days prior to effectuating any changes to its policy and procedure.

11) DHCS may request Contractor to make modifications with advance notice of a minimum of fourteen (14) business days.

12) Where technically and operationally feasible, Contractor must implement requested modifications within fourteen (14) business days of receiving such a request from DHCS. If technological or operational work is necessary to implement proposed modifications, Contractor may propose to DHCS, for approval, an alternate timeframe for implementation.

D. Contracts or Memoranda of Understanding (MOUs) with MCPs, LEAs and IHEs

1) If DHCS deems necessary, Contractor must enter into a contract or Memorandum of Understanding (MOU) with all participating MCPs, LEAs, and IHEs.

2) No later than thirty (30) calendar days after deemed necessary, Contractor must develop and submit to DHCS, for approval, a contract or MOU template for each entity type (MCP, LEA, IHE) that details the framework for collaboration and intended outcomes as it pertains to the duties and responsibilities of Contractor in its capacity as the single statewide third-party administrator for the CYBHI Fee Schedule Programs. At a minimum, the contract or MOU template must include:

a. Responsibilities for data oversight and processes among providers, payers, and the Contractor.

b. Responsibilities of LEAs and COEs for provider network reporting and credentialing (e.g., submitting provider/practitioner information)

c. Contractor’s operational structure, including after-hours policies and procedures and customer support.

d. Data and information exchange.

e. Reporting and quality improvement requirements.

Exhibit A
Scope of Work

f. Dispute resolution.

g. Member rights and grievances

h. Quality monitoring and oversight processes.

i. Other elements, as applicable

3) Data Use Agreement

a. Contractor must enter into a Data Use Agreement (DUA) with all participating MCPs, LEAs, and IHEs and is developing a DUA.

b. No later than thirty (30) calendar days following execution of this Contract, or a later date as agreed to in writing between DHCS and Contractor, the Contractor will review and agree as a participating entity to any Data Use Agreement (DUA) with providers and payers as determined necessary by DHCS, which will outline all aspects of how exchanged data will be used and will include requirements to maintain a data safeguard program to conform to data confidentiality and security requirements of DHCS policy and procedures and all relevant State and Federal requirements, including Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Act (FERPA) standards. Additional components of the DUA will include, but not be limited to, the following:

i. Data files

ii. Social Security Administration agreement

iii. Security provisions and controls

iv. Notification of breach

v. Certificate of destruction

vi. Other elements as determined by DHCS.

E. Data, Reporting and Evaluation Requirements

1) Contractor will collect, analyze, and transmit related to the provider network, claims, and payer and provider supports to DHCS in a manner, format specified by DHCS.

2) Contractor will implement data reporting processes to demonstrate performance outcomes, inform the CYBHI evaluation, create reporting dashboards.

Exhibit A
Scope of Work

3) Contractor must comply with all security and confidentiality requirements in accordance with the Contract, including Exhibit A and all associated attachments.

4) Contractor will participate in and contribute to activities related to the CYBHI evaluation, including participating in meetings with the CYBHI evaluation vendor, DHCS and CalHHS, as appropriate.

5) As directed by DHCS, Contractor will enable analyses across data sets by receiving, linking, consolidating, enriching, and storing data from both internal

    a. Internal DHCS databases (e.g., Short-Doyle/Medi-Cal Claim system for Medi-Cal reimbursement of services).

    b. County, state or federal databases (e.g., CalSAWS, a California based integrated statewide eligibility database for Medi-Cal for user eligibility verification or track overall changes such as school attendance, hospitalization rates and suicide rates).

    c. Partner databases (e.g., schools, community-based organizations).

    d. Business service databases (e.g., 3rd party behavioral health content library).

6) Contractor will work with other DHCS programs and any delegated contractor to define, identify, and document any additional data source that may be required to improve the insights offered.

7) Contractor will work in coordination with DHCS and the source system owner to detect and report data quality issues and consume only the quality data to maintain the integrity and accuracy of analytics and reporting.

8) Contractor will develop and maintain interfaces with identified and configured data sources through industry-standard data connectors (e.g., APIs).

9) Contractor will implement a data governance program approved by DHCS to ensure data is consistent, trustworthy and doesn’t get misused.

10) Contractor will monitor and make all reasonable efforts to ensure data compliance with all applicable laws, policies, procedures, rules, codes, and standards for data held or used by system(s) under Contractor’s responsibility.

Exhibit A
Scope of Work

11) Contractor will implement, monitor, and respond to data incidents in alignment with DHCS-approved security policies and procedures that affect data and information assets.

12) Contractor will enable a comprehensive data archival process, with the ability to archive and restore archive to the original state of reliability, compliant with DHCS standards.

13) Contractor will allow for data access for, and in compliance with, DHCS Data Policies and Standards and Federal and State laws and regulations of California (e.g., Data Source files, queries, administrative, quality/audit data, and analytics/reporting output).

14) Contractor will comply with data retention rules and controls according to DHCS approved policies and standards and Federal and State laws and regulations of California.

15) Contractor will establish a reporting and measurement process that will enable data collection and reporting capabilities spanning programmatic and DHCS operational functions with pre-developed and customized reports and dynamic dashboards.

16) Contractor will run pre-configured, on-demand reports, such as quantitative data analytics and historical reporting.

17) Contractor will safely ingest data from different data sources.

18) Contractor will minimize data errors (e.g., records duplication, overwriting, truncation, etc.).

19) Contractor will track metrics for data quality measurement such as accuracy, completeness, consistency, integrity, and timeliness on the data being used and consumed by the Contractor.

20) Contractor will maintain log files on all actual or attempted violations of security policies, practices, or procedures for data held or used.

21) Contractor will track data lineage with the ability to rollback data to a particular lineage version if needed.

22) Contractor will use data exchange mechanisms that are HIPAA, FERPA, and Interoperability and Patient Access compliant, if applicable.

23) Contractor will provide the ability to create and extract customized data sets.

24) Contractor will maintain all data, including but not limited to documents, administrative data, support data, billing data, and any data containing

Exhibit A
Scope of Work

Sensitive Information, always in servers located in the United States or in servers of which the operations and maintenance are subject only to the laws of the United States.

25) Contractor will support authorized and authenticated access to user data and outcome measures based on regulatory requirements and the needs of CYBHI stakeholders across DHCS, CalHHS, and strategic partners.

26) Contractor will support automation via workflows and identified capabilities that enable customized data handling and notification (e.g., data ingestion, data formatting, data presentation, automated alerting) for users.

27) Performance dashboards

a. No later than thirty (30) calendar days or a later date as agreed to in writing between DHCS and Contractor after execution of the contract, Contractor must submit to DHCS for approval a Data Management Plan that addresses, at a minimum, the following:

vii. Data Governance Approach

viii. Data Architecture Approach (e.g., including schemas)

ix. Data Storage & Operations Approach

x. Reference Data Approach

xi. Master Data Approach

xii. Data Quality Approach

xiii. Data Exchange and Integration Approach

xiv. Metadata Approach

xv. Data Warehouse Approach

xvi. Business Intelligence Approach

xvii. Data Security & Privacy Approach

xviii. Documentation on data mapping (source-to-target lineage) and sourcing strategy for any additional internal / external data elements.

b. On a monthly basis, beginning the first month of claims processing, Contractor must submit to DHCS a comprehensive, public-facing performance dashboard. Elements of the performance dashboard may include but are not limited to:

Exhibit A
Scope of Work

i. Provider Demographics: Comprehensive breakdown of providers by demographics such as specialty, location, gender, languages spoken, and years of experience;

ii. Provider Enrollment & Termination: List of providers/practitioners who have been added or terminated from the directory within a given timeframe;

iii. Provider Directory Accuracy Audit: Number of discrepancies or inaccuracies in provider/practitioner information compared against primary source verifications;

iv. Provider Outreach & Engagement: Outreach efforts to providers, such as training sessions, informational webinars, or communications;

v. Provider Feedback & Complaints: Number of feedback, complaints, or issues reported by providers;

vi. Utilization Report by Provider: Number of patients seen, services rendered, or procedures performed by each provider;

vii. Performance Metrics: Evaluation of providers based on performance metrics like patient satisfaction scores, quality of care metrics, or adherence to best practices; and,

viii. Directory Access & Usage: How often and by whom the provider directory is accessed.

ix. Claims Volume by LEA/IHE: The number of behavioral health claims submitted by each LEA/IHE;

x. Claims Approval & Denial Rates: Breakdown of the percentage of claims that are approved versus those denied (both initially and ultimately);

xi. Reasons for Claim Denials: The most common reasons for claims denial;

xii. Service Type Utilization: Claims by the type of behavioral health service provided (e.g., psychoeducation, case management);

xiii. Claim Turnaround Time: The average time taken from claim submission to approval or denial;

Exhibit A
Scope of Work

xiv. Claims Trend Over Time: Monthly or yearly trends in the number claims submitted;

xv. Claims by Service Type: Distribution of claims based on service type;

xvi. Billing Errors: Most common billing errors made in claims submissions;

xvii. Appeals & Resolutions: The number of appealed claims, reasons for appeals, and their resolution outcomes;

xviii. Claims by Age Group & Grade: Claims by students' age groups or grades; and,

xix. Pending Claims: Claims that are still in process.

xx. Other data elements required by DHCS, DMHC, CDI, CalHHS, or the Legislature.

F. Training and Technical Assistance

1) Contractor will lead and participate in training and technical assistance (TTA) activities for all participating entities (i.e., MCPs, LEAs, IHEs, designated providers and practitioners). TTA activities will focus on onboarding and ongoing support to providers and MCPs for provider network management, claims administration, and payment remittance functions. TTA activities include, at a minimum, cohort learning collaborative meetings, offices hours sessions, 1:1 technical assistance sessions.

2) Contractor may use various modalities for providing TTA including, but not limited to, the following:

a. Webinars

b. Learning collaborative workshops

c. 1-on-1 and group training sessions

d. E-mail inbox

e. Telephone helpline

f. Online courses

g. Others

3) Contractor will provide end-users with multiple channels or questions and issues resolution (e.g., telephone support line, e-mail inbox for support

services, chatbot/live chat accessible via Contractor's website or platform).

a. Contractor will adhere to response times as established by DHCS and agreed upon by Contractor across all support channels.

b. Contractor will provide an escalation mechanism to address any potential delayed responses to questions.

4) Contractor will regularly engage with stakeholders (e.g., payers, providers) to seek input about the processes associated with accessing and using the provider network and claims administration platforms.

5) Contractor will participate in all DHCS and/or CalHHS public webinars and workgroups, as applicable.

G. Implementation Plan and Project Management

1. No later than twenty-one (21) calendar days after contract execution, Contractor must submit to DHCS, for approval, a comprehensive Implementation Plan detailing Contractor's workplan, included associated timelines, for implementing all business requirements detailed in Exhibit A, including all attachments, of this scope of work. The Implementation Plan will include, at a minimum, the following:

   a) A comprehensive set of key timelines and milestones, including identifying dependencies across tasks to achieve milestones.

   b) A set of success metrics on which progress of implementation will be measured.

   c) A proposed schedule of required resources (e.g., personnel, technology) and how they would be utilized.

   d) A set of identified potential risks/challenges and corresponding contingency plans.

   e) A proposed TTA plan, which includes a proposed schedule for public webinars and technical assistance sessions (e.g., provider onboarding sessions, office hours).

   f) A proposed schedule of project team meetings with DHCS and its partners, as well as Contractor's project management framework and artifacts.

2. Contractor must maintain sufficient staffing to carry out its Implementation Plan, including timely submission of all deliverables and timely execution of business requirements, as specified in this Exhibit.

Exhibit A
Scope of Work

H. CYBHI DHCS Requested Consultants

1) Contractor will develop a standard contract and SOW subject to DHCS approval, that the Contractor will use to contract with the requested consultant(s). The standard contract will, at a minimum, outline the CBYHI program and the scope of work expected to be performed to ensure the successful implementation and use of the CBYHI statewide fee schedule.

I. Additional Requirements

2) Contractor will comply with all business requirements as specified and detailed in the additional Attachments to Exhibit A:

a. Exhibit A, Attachment I: Security and Confidentiality Requirements

b. Exhibit A, Attachment II: Turnover

6. Allowable Scope of Work Changes

A. The parties acknowledge that there are a significant number of details to be worked out following entry of the initial contract and SOW, and that changes to this scope of work may be required to account for information learned following entry into this agreement and/or as supplemental documents, processes, and policies related to the program are developed. If material changes to the program necessitate changes to the SOW, the parties agree to revise the SOW.

B. Contractor may request changes or revisions to the Scope of Work, and business requirements detailed herein, by submitting the request to DHCS in writing. All requested changes and revisions are subject to the prior approval of DHCS.

C. Within 15 business days of receipt of the Contractor’s request to change or revise this Scope of Work, or the business requirements herein, DHCS will respond, in writing, as to the approval or disapproval of all such requests. Should DHCS fail to timely respond to Contractor's written request, Contractor's request will be deemed approved.

D. The Contractor’s failure to obtain prior approval from DHCS for any deviations or changes to this Scope of Work, or the business requirements herein, may result in an audit finding and/or penalties and withholds, as specified in Exhibit B, Attachment I, Special Payment Provisions.

E. DHCS may require or request changes and/or revisions to the Scope of Work, or the business requirements herein. DHCS will make a good-faith effort to provide Contractor 30 calendar days advance written notice of said

Exhibit A
Scope of Work

changes or revisions. Such changes are subject to the prior approval of the Contractor, such approval not to be withheld without cause.

F. DHCS and Contractor may utilize a Work Order Authorization (i.e., a written request to specify or modify activities necessary to carry out this scope of work) to specify, on a quarterly or more frequent basis, ongoing activities and tasks necessary to carry out the services and deliverables detailed in this Scope of Work and the business requirements herein.

7. Records & Record Keeping

A. In Contractor will retain all financial records, supporting documents, statistical records, and all other records pertinent to the services provided in this Agreement.

B. DHCS or any of its authorized representatives, have the right to access any documents, papers, or other records of Contractor which are pertinent to this Agreement, for the purpose of performing audits, examinations, excerpts, and transcripts. The right to access records also includes timely and reasonable access Contractor's personnel for the purpose of interview and discussion related to the requested documents.

C. The right to access records is not limited to the required retention period but lasts as long as the records are retained by Contractor for a period of three (3) years from the date of submission of the last invoice.

8. Americans with Disabilities Act

Contractor agrees to ensure that deliverables developed and produced, pursuant to this Agreement will comply with the accessibility requirements of Sections 7405 and 11135 of the California Government Code, Section 508 of the Rehabilitation Act of 1973 as amended (29 U.S.C. §794d), regulations implementing the Rehabilitation Act of 1973 as set forth in Part 1194 of Title 36 of the Code of Federal Regulations, and the Americans with Disabilities Act of 1990 (42 U.S.C. §12101 et seq.). In 1998, Congress amended the Rehabilitation Act of 1973 to require Federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities. California Government Code Sections 7405 and 11135 codifies Section 508 of the Rehabilitation Act of 1973 requiring accessibility of EIT.

9. Executive Order N-6-22 – Russia Sanctions

On March 4, 2022, Governor Gavin Newsom issued Executive Order N-6-22 (the EO) regarding Economic Sanctions against Russia and Russian entities and individuals. "Economic Sanctions" refers to sanctions imposed by the U.S. government in response to Russia's actions in Ukraine, as well as any sanctions imposed under state law. The EO directs state agencies to terminate contracts

with, and to refrain from entering any new contracts with, individuals or entities that are determined to be a target of Economic Sanctions. Accordingly, should the State determine Contractor is a target of Economic Sanctions or is conducting prohibited transactions with sanctioned individuals or entities, that will be grounds for termination of this agreement. The State will provide Contractor advance written notice of such termination, allowing Contractor at least 30 calendar days to provide a written response. Termination will be at the sole discretion of the State.

10. GenAI Technology Use & Reporting

A. During the term of the contract, Contractor must notify the State in writing if their services or any work under this contract includes, or makes available, any previously unreported GenAI technology, including GenAI from third parties or subcontractors. Contractor shall immediately complete the GenAI Reporting and Factsheet (STD 1000) to notify the State of any new or previously unreported GenAI technology. At the direction of the State, Contractor shall discontinue the use of any new or previously undisclosed GenAI technology that materially impacts functionality, risk or contract performance, until use of such GenAI technology has been approved by the State.

B. Failure to disclose GenAI use to the State and submit the GenAI Reporting and Factsheet (STD 1000) may be considered a breach of the contract by the State at its sole discretion and the State may consider such failure to disclose GenAI and/or failure to submit the GenAI Reporting and Factsheet (STD 1000) as grounds for the immediate termination of the contract. The State is entitled to seek any and all relief it may be entitled to as a result of such non-disclosure.

C. The State reserves the right to amend the contract, without additional cost, to incorporate GenAI Special Provisions into the contract at its sole discretion and/or terminate any contract that presents an unacceptable level of risk to the State.

Exhibit A, Attachment I
Security and Data Requirements

I. Security and Confidentiality

A. Overview

1. Contractor must ensure compliance with all applicable state and federal laws and regulations, pertaining to confidentiality, integrity, and the availability of information that is received, created, processed, stored, and transmitted by Contractor as agreed upon within the Contract. Contractor will ensure security and confidentiality of all data, including all data and information defined in Exhibit D(S) and Exhibit H – Business Associates Addendum, regardless of transmission method or medium. Sensitive Information will include Confidential Information as defined in Exhibit D(S) Section 5, Protected Health Information as defined by HIPAA and the HITECH Act, and Personally Identifiable Information as defined by the California Privacy Rights Act, associated with the Contract.
2. The provisions in this Attachment supplement but do not replace or supersede, the provisions of Exhibit D(S), Special Terms and Conditions, Exhibit H, Health Insurance Portability and Accountability Act (HIPAA), Business Associate Addendum (BAA), and Exhibit I, DHCS Information System Security Requirements (ISSR).
3. The objectives of this Attachment are to:
    a) Protect the confidentiality, integrity and the availability of information that is received, created, processed, stored and transmitted by the Contractor as a result of this Contract.
    b) Protect the security and confidentiality of all data and Sensitive Information, regardless of storage, location or transmission method or medium, and all facilities, equipment and staff associated with this Contract.
    c) Ensure compliance with all applicable state and federal law statutes and regulations – including the HIPAA of 1996 regulations regarding security and privacy of Protected Health Information (PHI); OMB Circular A-130, National Institute of Standards and Technology (NIST) SP; and Exhibit H, HIPAA Business Associate Addendum (BAA).
    d) Ensure the submission and update of the System Security and Confidentiality Plan (SSCP) to demonstrate compliance with DHCS standards and Contract requirements. The SSCP will identify security controls, policies and procedures for the storage, processing and handling of all information (including Sensitive Information) by the Contractor and subcontractors, as

Exhibit A, Attachment I
Security and Data Requirements

well as the security of all staff; Contractor Facilities and equipment; storing, processing, or handling of data associated with this Contract.

e) Meet NIST 800-53 R5 Security and Privacy Controls for Information Systems and Organizations and establish a security and confidentiality training program that is specifically designed for all levels of Contractor staff, including subcontractors, providing services under the Contract and ensure compliance with DHCS standards and Contract requirements.

B. Requirements

1. General Requirements

a) Contractor must comply with the Security and Confidentiality requirements in this Attachment and will implement administrative, physical and technical safeguards that protect the confidentiality, integrity and availability of the public confidential, sensitive and personal information that is received, created, processed, stored and transmitted by the Contractor in connection with the Contract.

b) Within the earlier of ninety (90) business days after Contract execution, or prior to Contractor's first receipt, creation, processing, storage, or transmission of Sensitive Information in connection with the Contract, the Contractor will submit to DHCS for approval a System Security and Confidentiality Plan, Manuals and related documentation (collectively, the "SSCP") in accordance with standards and requirements in this section and Exhibit A – Scope of Work, and all Attachments to Exhibit A. These documents will be reviewed and updated through the term of the Contract and as requested by DHCS.

(1) The SSCP will include detailed standards and procedures to ensure adequate safeguards for the various operations related to those portions of the network not supported by the California Office of Technology Services (OTECH) as well as to prevent unauthorized disclosure of Sensitive Information.

(2) The SSCP will include standards and procedures for the following items:

(a) Identifying and marking of Sensitive Information as defined above.

(b) Storing of Sensitive Information, including custodial responsibility.

Exhibit A, Attachment I
Security and Data Requirements

(c) Access, retrieval, and duplication of Sensitive Information.
(d) Disclosure of Sensitive Information, including approving authority.
(e) Disposal of inactive Sensitive Information, including secure archives and shredding/pulverizing/melting.
(f) Compilation of a list of all classes and types of documents.
(g) Confidentiality classification criteria for each item on the compiled list from Section I.B.1.b.(2)(f) above.

(3) The SSCP will include standards and procedures for addressing the following potential categories of threats to Sensitive Information:
(a) Accidental disclosure, modification and/or destruction because of hardware error, process error, human error, or any combination of these.
(b) Casual access, resulting in unauthorized disclosure, modification and/or destruction by, but not limited to:
(i) Non-technical persons such as terminal operators, support staff, janitors, maintenance workers, vendors or subcontractors.
(ii) Skilled technicians such as operations staff, or others who have significant expertise in all process areas.
(iii) Managers, supervisors, and others with authorized access.
(iv) Premeditated criminal acts.
(v) Natural disasters.
(vi) Labor strikes.

(4) The SSCP will identify all transportation and data holding resources, both temporary and permanent, used by the Contractor and the Facilities, if any, which handle both electronic and/or hard copy data.
(5) The SSCP will address compliance with the authorities cited in the General Requirements Section of this Attachment.

Exhibit A, Attachment I
Security and Data Requirements

(6) The SSCP will include procedures and set safeguards to protect against possible collusion between Contractor employees and any other party, as well as safeguard against other potential security breaches.

c) Unless required earlier by applicable law, on the later of the Launch Date or within thirty (30) days of receipt of DHCS approval, Contractor will implement the SSCP.
d) The Contractor will comply with the Security and Confidentiality standards identified in this Contract, and, upon DHCS' approval, meet all deadlines established in the Contractor's SSCP.
e) All electronic media transmissions of Sensitive Information will be encrypted using Transport Layer Security (TLS) 1.3 encryption for Sensitive Information in transit and Advanced Encryption Standard (AES) 256 for Sensitive Information at rest, or other industry-standard protection approved by DHCS in writing.
f) If a subcontractor performs work on behalf of the Contractor, the Contractor will require the subcontractor to comply with all applicable requirements set forth in this Attachment.
g) In the event of a Data Breach (as defined by HIPAA) or Security Incident (as defined in the BAA), the Contractor will take the steps outlined in Exhibit H, HIPAA BAA.
h) All procedures, deliverables and/or related documentation required in this Attachment will be developed and formally submitted timely to DHCS for review and written approval, which will not be withheld without reasonable cause (e.g., documentation does not demonstrate compliance with the requirements herein), prior to implementation. DHCS will respond with an outcome within ten (10) business days of submission. Only material changes to documentation will require further approval from DHCS.
i) On or before the Launch Date, unless required earlier by applicable law, all processes, procedures, standards, documents and deliverables will be compliant with, as applicable, the following applicable authorities, including, but not limited to, as directed by DHCS and as needed to ensure compliance with standards:
    (1) Office of Management and Budget (OMB) Circular A-130,
    (2) NIST 800 Series Publications, specifically NIST 800-53 R5,

Exhibit A, Attachment I
Security and Data Requirements

(3) 45 Code of Federal Regulations, Section 205.50,
(4) California Public Records Act (California Government Code §7920.000 et seq.),
(5) Welfare and Institutions Code Sections 10850, 10850.1, 10850.2 and 14100.2,
(6) Title 22, California Code of Regulations, Section 51009,
(7) California State Administrative Manual (SAM), Section 5300-5399,
(8) Information Practices Act of 1977 (Civil Code §1798 et seq.),
(9) Confidentiality of Medical Information Act (California Civil Code §56 et seq.),
(10) The Health Insurance Portability and Accountability Act of 1996 (HIPAA),
(11) California Consumer Privacy Act (CCPA).
(12) Children's Online Privacy Protection Act of 1998 (COPPA).
(13) NIST 800-53 R5 Security and Privacy Controls for Information Systems and Organizations and Federal Risk and Authorization Management (FedRAMP) (moderate impact level) for cloud environments and services (i.e., Contractor's cloud hosting vendor partner must be certified as compliant with FedRAMP moderate impact level).
(14) Federal Information Processing Standards (FIPS) Publications,
(15) Department of Health Care Services (DHCS) Security and Confidentiality Standards,
(16) DHCS Information System Security Requirements (ISSR),
(17) Federal Information Security Management Act (FISMA) Compliance,
(18) DHCS Data De-identification Guidelines (DDG) v2.2 (https://www.dhcs.ca.gov/dataandstats/Pages/PublicReportingGuidelines.aspx), and
(19) Other requirements of California and federal law, including related regulations and published guidelines, to the extent that these authorities contain requirements applicable to the Contractor's performance under this Contract.

Exhibit A, Attachment I
Security and Data Requirements

j) The SSCP will be applicable to all employees and subcontractors providing services in connection with the Contract and to all Contractor Facilities (as defined below) and equipment storing, processing, or handling Sensitive Information.

2. Security and Confidentiality Requirements
   a) Compliance Assessment:
      (1) At a minimum, on an annual basis, and upon DHCS' reasonable request (e.g., as necessary to ensure compliance), the Contractor will conduct a compliance assessment to demonstrate compliance with new state and/or federal requirements. The assessment and supporting documentation will be formally submitted to DHCS for review and approval, which will not be withheld without reasonable cause. The requirement will be considered met once the Contractor receives formal written approval from DHCS.
   b) Facility Requirements
      (1) Facility will mean a physical location owned or leased, and occupied, by Contractor which stores physical copies of Sensitive Information, or which houses Contractor's servers which store electronic copies of Sensitive Information. For the avoidance of doubt, Facility will not include shared workspace(s) or remote worker locations. To the extent a Facility meets the foregoing definition, the Facility will include, but not be limited to the computer room, software and data libraries, data preparation areas, job entry and programming areas, mail room/pickup areas, record retention sites, computer terminals (on/off- site), telephone room and any junction boxes between telephone room and computer room, and safe storage vaults (on/off-site).
      (2) Upon reasonable notice (two (2) business days or more), permit authorized DHCS staff access to any Facility or equipment storing, processing or handling Sensitive Information covered by this Contract. For equipment containing Sensitive Information maintained at remote, non-Facility locations, Contractor will arrange for DHCS' access within a reasonable timeframe, including unannounced inspections where DHCS have significant concerns about the security of data and monitoring activities, as applicable. Such access will be at the discretion of DHCS as described

Exhibit A, Attachment I
Security and Data Requirements

in Exhibit E, Additional Provisions, unless applicable law grants independent access to representatives of other DHCS and federal agencies.

(3) Secure all Contractor Facilities, if any, including disaster back-up sites, so that only authorized persons are permitted entry into the Facility, and that such persons are restricted to those areas that they are permitted to access. Access control requirements will include:

(a) Facility entry and control points will be locked or guarded at all times. An up-to-date copy of the security policy must be maintained in the Facility, and its location and contents made aware to all Contractor staff at the Facility.

(b) The Contractor will obtain a written certification that is signed by each Contractor staff at the Facility that he/she has reviewed and will comply with the security policy, including all new material that has been updated or deleted, and provide such certification to DHCS upon request.

(c) The Contractor will run a monthly status report to ensure that all cards with no activity in a month's time are deactivated unless explicitly authorized by DHCS or Contractor's management. Control points will be established for each of the following areas, if applicable: main entrance to the Facility(ies), service entrance(s), loading platform(s), garage entrance(s); inside entrance to the Facility(ies), and secondary entrance(s).

(d) The Facility(ies) will be monitored by security cameras twenty-four (24) hours per day, seven (7) days a week, including State holidays, unless otherwise directed by DHCS.

(e) The Contractor staff will be responsible for entry into the Facility(ies) between the hours of 8:00 a.m. and 5:00p.m. PST, in the applicable time zone, Monday through Friday. The Contractor staff will be responsible for the issuance and monitoring of Facility badges and contacting the appropriate staff for escorting guests into the Facility(ies).

(f) The security cameras will record vulnerable areas, including but not limited to, if applicable: the

Exhibit A, Attachment I
Security and Data Requirements

reception area(s); all outside entrances to the Facility(ies); inside entrances, if other Contractor accounts are served from the same location; loading docks and garages; operations Facilities/rooms; and on/off-site vault storage areas. The Contractor will audit the security footage randomly monthly, or with respect to specific times or footage, for reason as reasonably determined by Contractor, DHCS, or as required by law. The recorded information for each twenty-four (24) hour period will be logged and kept for a minimum of one-hundred eighty (180) calendar days from the date recorded. A copy of the recorded information, in a media determined by DHCS will be provided to the DHCS within twenty-four (24) hours of request, subject to confidentiality restrictions.

(g) Upon change of duty or termination of Contractor staff or subcontractors, access authority will be updated or removed immediately, and Contractor staff will escort the employee or subcontractor from the Contractor's premises, if applicable. Employees or subcontractor will not be allowed to return to a Facility unescorted after termination of employment or subcontract or change of duty triggering removal of access.

(h) Require a badge, with a recent photo, and key card system using a two (2)-factor authentication system, for staff. Staff badges will denote the level of access allowed to the individual. Temporary badges will be required for visitors. Visitor badges will denote whether escort by Contractor or authorized DHCS staff is required. The key card for all Contractor staff and visitors will be re-coded every six (6) months throughout the Contract term, unless the Contractor proposes and DHCS accepts an equivalent system that will provide equal protection for the Facility(ies) environment.

(i) If applicable, log the entry and exit of visitors and messengers by visitor name, agency represented, date and time of arrival and departure, telephone

Exhibit A, Attachment I
Security and Data Requirements

number, and name of individual to whom the visit is made. Identification and/or credentials of all visitors and messengers will be verified and validated. Visitors and messengers will be given badges and escorted to their destination by the Contractor staff or DHCS employee, if applicable. All temporary badges will be monitored, tracked and retrieved from visitors and messengers upon their departure and the entry log updated. The entry log will be audited regularly. The Contractor will, at the end of each business day, disable all temporary access badges that are not returned at the end of that business day. The Contractor will not issue any temporary badge on a permanent basis to any entity. A copy of the entry log will be submitted to the DHCS on a monthly basis.

(j) If applicable, secure and lock the telecommunications area and any junction boxes between the telephone room and the operations room at all times with key control under the supervision of the building and/or data processing management.

(k) If applicable, secure and lock the operations and equipment room/Facilities at all times. Access must be monitored and auditable (i.e., use of individual access cards).

(l) If applicable, protect the Facility(ies) against intrusion with a surveillance alarm extended to a manned monitoring center.

c) Other Security Measures. On or before the Launch Date, unless required earlier by applicable law, Contractor will use required state, federal and industry best practices to:

(1) Protect all Sensitive Information, whether hard copy or electronic copy, to prevent unauthorized access.

(2) Ensure only authorized persons may access in accordance with a person's duties (role-based access), the following:

(a) Sensitive or confidential information and PHI.

(b) Process programs and process documentation, including procedure manuals.

Exhibit A, Attachment I
Security and Data Requirements

(c) Operations room, information libraries, and vaults, if applicable.

(3) Upon employee termination, layoff notification or change of duty triggering removal of access, Contractor will immediately revoke access to all systems/applications.
(4) Protect every automated file, relating to this contract, containing Sensitive Information by the Resource Access Control Facility (RACF)/Access Control Facility/2 (ACF/2), or equivalent software, to prevent unauthorized access.
(5) Require passwords to access Contractor functions and/or any associated applications via computer terminal.
(6) Establish a Network Access Help Desk to assist authorized users in resolving password/access inquiries. Upon request from an authorized user, in writing, the Contractor will reset expired passwords or resolve other password problems.
(7) If at any point during the Term, Contractor handles physical Sensitive Information Contractor will develop and submit to DHCS for approval, procedures for the handling, packaging, and transportation of physical Sensitive Information. The procedures will protect against unauthorized access. The Contractor will use a secure service when transporting any document(s) or report(s) or any other type of media that contains Sensitive Information, approved by DHCS.
(8) If applicable, provide a scalable solution for the telecommunications links among the California Office of Technology Services primary and secondary sites and the primary and secondary sites.
(9) Implement a solution that tracks the electronic system access for applicable employees including Contractor and State employees. Applications to be tracked to the extent applicable to services under the Contract, include, but are not limited to, and all subsystems, State Fair Hearings, Project Management System, Document Management System, Electronic Imaging Management Systems and any other applications that contain

Exhibit A, Attachment I
Security and Data Requirements

Sensitive Information. The solution must be able to report the following at a minimum:
(a) Employee name.
(b) Date and time access was granted.
(c) Name of system(s)/application(s).
(d) Access level granted.
(e) Access changes (including system, date/time, access level).
(f) Person granting the access or modifying the access (including revoking access).

(10) Implement a solution to enable:
(a) A Host-Based Intrusion Detection System (HIDS) that integrates, if applicable, with the existing Medi-Cal environment on Department servers containing Medi-Cal information.
(b) Internet Protocol (IP) source filtering to allow only authorized network access to database servers containing Sensitive Information.
(c) Server-hardening standards for all existing and new servers to include HIDS congruent with the DHCS Information Security Office standards.

(11) Implement a solution that provides for:
(a) Securing and Encrypting email communications.
(b) Database client authentication.
(c) Appropriate logging and auditing.
(d) Specific security enhanced modifications, as described in this Attachment.
(e) Includes validation mechanism that verifies with the original sender all new email addresses registered from their e-mail.

(12) If applicable, implement a solution in place that provides for secure transfer of data between the data centers, the Contractor and OTECH data centers. Solution must comply with standards and contract requirements.

3. Risk Analysis/Assessment Requirements
a) In order to ensure that all data, hard copy or electronic, including Sensitive Information, will remain secure and confidential, the Contractor will perform an analysis of the risks that exist to keep that information private.

Exhibit A, Attachment I
Security and Data Requirements

b) The Contractor will:
   (1) Submit a Risk Analysis/Assessment report for DHCS review and approval, which will not be withheld without cause, in accordance with requirements in Exhibit A – Scope of Work, annually through the term of the Contract and as reasonably requested by DHCS.
   (2) Perform and document a detailed Risk Analysis/Assessment report, which defines all risks associated with collection, storage, processing, transition, transportation, discarding or use of Sensitive Information under this Contract. This analysis/assessment will be completed by a third party or by Contractor staff independent from the Contractor operations staff, such as the appropriate Information Security Office, Privacy Office or Auditing staff, and reviewed/approved by the Contractor's Information Security Officer and Privacy Officer prior to submission to the DHCS.
   (3) Provide a Corrective Action Plan with the Risk Analysis/Assessment report that contains timeframes for implementing the appropriate administrative, physical, and technical safeguards, as needed.
   (4) Ensure the Risk Analysis/Assessment report be submitted as a separate document.
   (5) Ensure appropriate and applicable backup documentation and safeguard review materials are delivered to the DHCS simultaneously with the Risk Analysis/Assessment report. Annually, or as the Contractor or DHCS deem necessary to ensure compliance with standards, Contractor will perform additional Risk Analyses/Assessments; review implemented safeguards; and modify, add, or delete safeguards as the need arises and as DHCS requests.
   (6) Perform a risk analysis and submit a Risk Analysis/Assessment report and a Corrective Action Plan for each identified issue to the DHCS no later than fifteen (15) business days after written request from DHCS and/or Contractor identification of the risk.

Exhibit A, Attachment I
Security and Data Requirements

4. Security and Confidentiality Training Program Requirements
   a) The Contractor will:
      (1) Establish a security and confidentiality training program as part of the System Security and Confidentiality Plan that is specifically designed for all levels of members of Contractor's workforce, as defined in 45 CFR 160.103 and including all employees and subcontractors performing services under the Contract. All persons and all Contractor staff having responsibility for data processing equipment and/or the handling or processing of, or the exposure to Sensitive Information will participate. Such training will occur no later than two weeks after the Department's approval of the training program. Once fully established and presented, an annual training program for all applicable staff will be maintained to ensure a continual awareness of security and confidentiality requirements. Additionally, new employees performing services under the Contract will receive security and confidentiality training within one work week (five business days) of their start date or before they are given any exposure to Sensitive Information. The training will cover a full range of security and confidentiality concerns including, but not limited to:
         (a) Definition of Sensitive Information and examples of the various types, both paper and electronic.
         (b) Federal and State law pertaining to Sensitive Information; (Health Insurance Portability and Accountability Act (HIPAA), Information Practices Act, W&I Code section 14100.2, National Institute of Standards and Technology (NIST), etc.
         (c) Staffs' ongoing responsibility to protect against unauthorized disclosure, with practical and realistic examples as to how such disclosure can occur, and what actions will be taken by all applicable staff to minimize or preclude the occurrence of unauthorized disclosure.
         (d) Both manual and automated processes to protect Sensitive Information from unauthorized disclosure and the procedures that have been developed to protect these processes.

Exhibit A, Attachment I
Security and Data Requirements

(2) If applicable, ensure all Contractor staff having access to DHCS data and/or networks, if any, attend DHCS' Information Security Training annually. Failure to complete such training will result in the employee having access revoked until such requirements are met. Any employees found to be in serious violation of the policies set forth in this Contract, as well as the directives set forth in the DHCS training course, will have access revoked indefinitely. All changes in employee status (e.g., new hires, promotions, or separations) for employees with access to DHCS data and/or networks must be reported to the Contracting Officer immediately.

(3) Submit annually, a report documenting employee attendance at Security and Confidentiality Training during the previous year. This report must include, at minimum:
   (a) Employee name.
   (b) Contractor's section/unit employee works in.
   (c) Date of last training.
   (d) Due date for next training.
   (e) The report must reflect if the employee is overdue for training and identify reasons for delays in training or non-attendance.

(4) Ensure that the contents of this Attachment are included in the standard language of any subcontract entered into to perform work arising from or related to this Contract, including completion and approval of the BAA by the DHCS and all parties with access to Sensitive Information.

(5) Submit documentation acceptable to DHCS to demonstrate compliance with security and confidentiality requirements and certification, in writing, that all requirements of this section have been, and will continue to be met, throughout the term of the Contract.

Exhibit A, Attachment I
Security and Data Requirements

5. Information Security/Privacy Office Requirements
    a) Overview
        (1) The Information Security/Privacy Office provides oversight of the Contractor's Information Security Program and Contractor's Privacy Program. These programs encompass all systems storing, processing, or handling Sensitive Information (i.e., automated and manual, physical and logical).
    b) Staff Requirements
        (1) The Contractor will employ an Information Security Officer and Privacy Officer to manage the Information Security/Privacy Office.
        (2) The Information Security Officer and Privacy Officer will be full time, dedicated employees of Contractor.
        (3) After execution of this Contract, any new Contractor staff identified in this section will require DHCS approval prior to working on behalf of the state of California, pursuant to this Contract.
    c) Office Requirements
        (1) The Contractor will, for the term of the Contract, establish and maintain an Information Security and Privacy Office.
        (2) The established Information Security and Privacy Office will properly execute the functions of the Information Security and Privacy Office as intended by the terms and conditions throughout this Contract.
        (3) The Information Security/Privacy Office duties will include, but are not limited to:
            (a) Develop security policies, procedures, and criteria for the collection, storage, access, and destruction of information assets. The policies and procedures provide the operational guidelines and delineate the roles and responsibilities of the Contractor's entities for assuring the security and integrity of information assets.
            (b) Develop or update required reports, manuals and related documentation.

Exhibit A, Attachment I
Security and Data Requirements

6. Reporting Requirements
    a) The Security and Confidentiality specific reporting requirements identified in this Attachment will comply with general reporting provisions specified in Exhibit A – Scope of Work. The following are the minimum reporting requirements for the requirements specified herein. DHCS reserves the right to reasonably request additional reporting or updates to existing reports throughout the Term of the Contract.
        (1) The Contractor will submit a Security and Confidentiality Report (S&CR) report on a monthly basis. The report will include, at a minimum, the following information:
            (a) Total number of threats to Sensitive Information by accidental disclosures, modifications and/or destruction.
            (b) Total number of threats to Sensitive Information by casual access, resulting in unauthorized disclosure, modification and/or destruction.
            (c) Total number of threats to the security of the facility(ies), if applicable.
            (d) Threats made, by type.
            (e) Total number, by type, of authorized personnel or entities with approved access to all facilities, equipment and related materials pursuant to this Contract, if applicable.
            (f) A summary of the video surveillance auditing required by this Attachment, if applicable.
            (g) A comprehensive overview of current and planned Security and Privacy activities for DHCS to use in oversight agency reporting.
            (h) A detailed and dashboard summary for all activities that are a result of an audit conducted pursuant to this Exhibit A, Attachment IV.
        (2) The Contractor will submit a report on a bi-annual basis identifying all current and authorized staff and their levels of access to the operational Facility(ies), if any, and to specific areas of information based on job assignment.

Exhibit A, Attachment I
Security and Data Requirements

(3) The Contractor will, on a monthly basis, submit to DHCS for review and approval a Plan of Action and Milestones (POAM) document as defined by DHCS standards.

C. Manuals and Related Documentation
1. Development and Maintenance
a) The Contractor will develop manuals and related documentation at any time throughout the term of the Contract to facilitate operations in accordance with the Contract. Manuals and related documentation may be created:
(1) At any time, upon DHCS' reasonable request.
(2) At any time, if the need is identified and DHCS approves the creation of the manual or document, which approval will not be withheld without cause.
(3) As necessary if technical, operational or procedural change requires the creation of a manual or document.
b) Unless otherwise specified, the Contractor will formally submit initial manuals and related documentation required by or created pursuant to this Attachment to DHCS for review and approval, which will not be withheld without cause, in accordance with the requirements in Exhibit A – Scope of Work.
c) The Contractor will review manuals and related documentation and submit updated copy(ies) to DHCS for review and approval if material updates are made, which approval will not be withheld without cause:
(1) Annually, throughout the term of Contract.
(2) At any time, upon DHCS' reasonable request.
(3) As necessary if material technical, operational or procedural change requires manual or documentation update.
d) If during the annual review or the DHCS requested review, the Contractor determines no updates are needed; certify to DHCS the manual or related documentation is complete and up to date.
e) The review certification will include a summary of all manuals and related documentation reviewed with a notation if the item is new for this review cycle, has been updated in the review cycle or is complete and up to date.

Exhibit A, Attachment I
Security and Data Requirements

2. Manuals and Related Documentation
    a) The list of manuals and related documentation identified in this Attachment will be considered the minimum required. The list will be updated through the term of the Contract.
    b) The following are Security and Confidentiality manuals and related documentation:
        (1) System Security and Confidentiality Plan.
        (2) Risk Analysis/Assessments.
        (3) Reports identified in the above Reporting Requirements Section.

II. Additional Data Analytics and Reporting Requirements

A. Contractor will collect, analyze and transmit user-level and population-based data to DHCS in a manner, format specified by DHCS.

B. Contractor will comply with the following requirements as it relates to analytics and reporting in accordance with the Contract.

C. DHCS owns and has all rights to data for users and claims resulting from this contract. Contractor will provide data to DHCS, and its designees (as applicable and with prior approval of DHCS) at no cost.

D. Contractor will not use or share data, related to this Contract, for any reason not specified in this contract and/or without prior approval from DHCS. Contractor will not, under any circumstances, sell any data related to this Contract.

1. Contractor will maintain all data servers, if any, in a physical location within the contiguous United States and in compliance with state and federal laws.

2. Contractor will ensure that access to User data (whether anonymized or not) is limited to individuals residing and located within the contiguous United States. Contractor support staff residing outside the United States will not have access to User data save for aggregated user data required for administrative or research purposes, subject to security requirements as outlined in this Attachment IV.

Exhibit A, Attachment I
Security and Data Requirements

3. As directed by DHCS, enable analyses across data sets by receiving, linking, consolidating, enriching, and storing data from both internal to state government (e.g., DHCS, CalHHS, etc.) and external sources, including but not limited to:

a) Internal DHCS databases (e.g., Short-Doyle/Medi-Cal Claim system for Medi-Cal reimbursement of services).

b) County, state or federal databases (e.g., CalSAWS, a California based integrated statewide eligibility database for Medi-Cal for user eligibility verification or track overall changes such as school attendance, hospitalization rates and suicide rates).

c) Partner databases (e.g., schools, community-based organizations).

d) Business service databases (e.g., 3rd party behavioral health content library).

e) Non-user inputted data (e.g., engagement metrics, feature utilization, user flow navigation flows).

4. Work with other DHCS programs and any delegated contractor to define, identify, and document any additional data source that may be required to improve data insights.

5. Work in coordination with DHCS and the source system owner to detect and report Contractor's data quality issues and consume only the quality data to maintain the integrity and accuracy of analytics and reporting.

6. Develop and maintain interfaces with identified and configured data sources through industry-standard data connectors (e.g., APIs).

7. Implement a data governance program approved by DHCS to ensure data is consistent, trustworthy and doesn't get misused.

8. Monitor and make all reasonable efforts to ensure data compliance with all applicable laws, policies, procedures, rules, codes, and standards for data held or used by system(s) under Contractor's responsibility.

9. Implement, monitor, and respond to data incidents in alignment with DHCS- approved security policies and procedures that affect data and information assets.

Exhibit A, Attachment I
Security and Data Requirements

10. Enable a comprehensive data archival process, with the ability to archive and restore archive to the original state of reliability, compliant with state law.

11. Upon reasonable request, allow for data access for, and in compliance with, DHCS Data Policies and Standards and Federal and State laws and regulations of California (e.g., Data Source files, queries, administrative, quality/audit data, and analytics/reporting output).

12. Comply with data retention rules and controls according to DHCS approved policies and standards and Federal and State laws and regulations of California.

13. Establish a reporting and measurement process that will enable data collection and reporting capabilities spanning programmatic and DHCS operational functions with pre-developed and customized reports.

14. Run pre-configured, reports, such as quantitative data analytics and historical reporting.

15. Safely ingest data from different data sources.

16. Minimize data errors (e.g., records duplication, overwriting, truncation, etc.).

17. Track metrics for Contractor's data quality measurement such as accuracy, completeness, consistency, integrity, and timeliness on the data being used and consumed by Contractor.

18. Maintain log files on all actual or attempted violations of security policies, practices, or procedures for data held or used by Contractor.

19. Track data lineage with the ability to rollback data to a particular lineage version if needed.

20. Use data exchange mechanisms that are HIPAA and Interoperability and Patient Access compliant, if applicable.

21. Maintain all data, including but not limited to documents, administrative data, support data, billing data, and any data containing Sensitive Information, always in servers located in the United States or in servers of which the operations and maintenance are subject only to the laws of the United States.

Exhibit A, Attachment I
Security and Data Requirements

E. Prior to launch of claims processing and no later than forty-five (45) days after contract execution, Contractor must provide a data management plan that covers the following areas:

1. Data Governance Approach
2. Data Architecture Approach (e.g., including schemas)
3. Data Storage & Operations Approach
4. Reference Data Approach
5. Master Data Approach
6. Data Quality Approach
7. Data Exchange and Integration Approach
8. Metadata Approach
9. Data Warehouse Approach
10. Business Intelligence Approach
11. Data Security & Privacy Approach
12. Documentation on process for data mapping, in the event that it is required in the future.

Exhibit A, Attachment II
Turnover Responsibilities

I. General Requirements

A. Contract Extension Option

1. DHCS may exercise an option to extend this Contract beyond the Contract Termination Date (CTD) through a mutually agreed upon amendment to the Contract, which will contain terms regarding the period of Contract extension and payment schedules for the same. If DHCS exercises its option to extend this Contract beyond the CTD, it will notify Contractor of the same in writing no less than twelve (12) months prior to CTD.
2. If DHCS exercises its option to extend this Contract beyond the CTD, the Turnover period will be delayed for a commensurate period-of-time.
3. If DHCS elects not to exercise this option, for a reason unrelated to continued fiscal appropriation in the California State Budget, DHCS will notify Contractor, in writing, twelve (12) months prior to CTD.
4. If DHCS elects not to exercise this option for a reason related to continued fiscal appropriation in the California State Budget, DHCS will, if possible, notify Contractor, in writing, at least six (6) months prior to CTD.

B. Maintenance of Operations

1. Contractor will continue to meet all Contract requirements until DHCS determines, in writing, that all fee schedule operations have been fully and successfully turned over to a successor contractor and/or DHCS; provided that, such obligations will not extend beyond the CTD unless such extension is mutually agreed between the parties. To the extent that an extension is required to allow Contractor to complete the activities required as part of the Turnover Phases specified in this Attachment V., Contractor will promptly seek such an extension. Payment for completion of activities specified in this Attachment V. will be made in accordance with Exhibit B, and such Payment will be considered payment in full.
2. The functions that will continue without interruption or modification until final turnover of operations, subject to section B.1. above, include, but are not limited to, the following:
    a) Maintenance and operations of the provider network and claims administration under the fee schedule in accordance with Exhibit A, including all attachments to Exhibit A, and the DHCS-approved operating model.
    b) Continued delivery of all provider network and claims administration capabilities, as specified in Exhibit A and Attachment I.
    c) Continued compliance with performance and security standards.

d) Maintenance of sufficient staffing levels in compliance with service level agreements.

e) Maintenance of partnership agreements and third-party contracts as necessary to deliver on the foregoing obligations.

f) Continued performance against key performance indicators, as specified in Exhibit A, including all attachments to Exhibit A, and Exhibit B, Attachment I, Special Payment Provisions.

g) Continued compliance with quality assurance, data collection and reporting requirements in accordance with this Contract and the DHCS-approved data reporting plan.

h) Continuation of weekly project team meetings with DHCS.

i) Participation in stakeholder events, evaluation meetings, and other DHCS or CalHHS meetings, as applicable.

j) Any and all other activities reasonably required to maintain the provider network and claims administration processes and/or as reasonably specified by DHCS.

3. Unless otherwise specified, required deliverables that are unrelated to Turnover, but which have submission dates during Turnover, will continue to be submitted on schedule. The inception of Turnover will not itself affect the submission of any non-Turnover related deliverables. Contractor may request that DHCS waive one or more deliverable requirements that are unrelated to Turnover, which request will not be denied without cause, but submission of all such deliverables will continue on-schedule unless or until DHCS issues a formal written response to Contractor's waiver request. DHCS will respond to all such requests within ten (10) business days of receipt of Contractor's request.

II. Turnover Phases

A. There will be four phases of Turnover:

1. Commencement
2. Procurement support and successor assumption of operations
3. Transfer of responsibilities
4. Last day of operations (LDO) and closeout

Exhibit A, Attachment II
Turnover Responsibilities

B. Commencement

1. If the Contractor determines it does not wish to continue TPA operations, Contractor will notify DHCS immediately and no later than fifteen (15) months prior to the Contract termination date (CTD) specified in this agreement or subsequent amendments.
2. Commencement of Turnover activities will begin immediately upon notification of the Contractor's intent to DHCS.
3. Contractor will comply with all requirements, activities, due dates, and quality assurance levels necessary to perform Turnover activities for the transfer of the responsibilities in this Contract to a successor contractor and/or to DHCS in the period leading up to the Contract Termination Date (CTD).
4. Contractor will make all reasonable efforts to ensure a smooth transition of operations to the successor contractor and/or DHCS, as applicable.
5. Within thirty (30) business days of Turnover notification, Contractor will submit to DHCS for approval a Turnover Plan that specifies key milestones, timelines, and deliverables in each phase.
6. Dates, frequencies, and/or timeframes stated in Exhibit A – Scope of Work, Attachment V – Turnover or the Turnover Plan may need to be adjusted to accommodate changing circumstances during the Turnover process. Any changes to dates, frequencies, or timeframes must be approved, in writing, by DHCS prior to implementation.
7. Turnover meetings and Turnover personnel
    a) For any meetings related to Turnover activities that are attended by both DHCS and Contractor staff, Contractor will:
        i. Create and distribute meeting artifacts by 10:00 a.m. PT, 1 business day prior to meeting or as directed by DHCS.
        ii. Record decisions, discussions, and action items, and distribute to all invitees and attendees within one (1) business day of meeting.
    b) Contractor will appoint a Turnover project manager to oversee all Turnover activities and to serve as a liaison between Contractor, DHCS, and the successor contractor. The individual will be dedicated and available, as needed, to fulfill Turnover responsibilities for the entire Turnover period. The Turnover Project Manager will be responsible for ensuring that all Turnover requirements are met and will serve as the Contractor's liaison to DHCS for the entire Turnover period.
    c) Contractor will designate one (1) individual as the Information Security Officer (ISO) to ensure continued compliance with Security and Data requirements, as specified in Exhibit A, Attachment I.

d) Contractor will designate one (1) individual as the Privacy Officer (PO) to ensure continued compliance with Security and Data requirements, as specified in Exhibit A, Attachment IV.

8. No later than thirty (30) days after notification to DHCS and initiation of Commencement activities, Contractor will create and submit to DHCS for review and approval a Turnover Risk and Issue Management Plan. DHCS will approve or request modifications to the Turnover Risk and Issue Management Plan within ten (10) business days of receipt from Contractor.
    a) Contractor will submit any updates to the Turnover Risk and Issue Management Plan to DHCS for review and approval.
    b) At DHCS' reasonable request anytime during Turnover, Contractor will review and update the Turnover Risk and Issue Management Plan and submit to DHCS for review and approval.
    c) The Turnover Risk and Issue Management Plan will be maintained through the Post-LDO and Turnover Closeout Phase.
    d) Any updates to the Turnover Risk and Issue Management Plan will be based on industry best practices.
9. No later than thirty (30) days after notification to DHCS and initiation of Commencement activities, Contractor will implement a Turnover Risk and Issue tracking and reporting system.
    a) Risk and Issue reporting will be part of weekly Turnover project meetings.
    b) Contractor will submit the final version of the Turnover Risk and Issue tracking and reporting system during Turnover Closeout.

C. Procurement support and successor assumption of responsibilities
1. Within ten (10) business days of Turnover notification and commencement, Contractor will provide to DHCS a draft Request for Proposals, outlining the key elements and capabilities required of a successor vendor.
2. Turnover Administrative Procedures Manual
    a) 12 months prior to LDO and monthly through LDO, the Contractor will submit to DHCS for review and approval a Turnover Administrative Procedures Manual.
    b) This manual will document the administrative procedures that will be performed to affect a smooth, problem-free turnover of Contract Operations to the successor contractor.
    c) This manual will include, but not be limited to those Contract requirements as stated throughout this Contract, including those in the Additional

Provisions and Special Terms and Conditions sections, budgets and finance, personnel, and operations.

d) Any updates made to the Turnover Administrative Procedures Manual from the prior submission must be clearly identified through a revision log and revision marks.

D. Transfer of responsibilities

1. Before any transfer of responsibilities, sharing of any proprietary information, or access to Contractor or DHCS intellectual property, any DHCS successor contractor will be required to sign a non-disclosure and confidentiality agreement, attest to the sublicensing limitations contained in Exhibit D(S), and demonstrate internal firewalls and protocols to ensure the sublicensing limitations in Exhibit D(S) will be honored.
2. Upon DHCS-identification of a successor contractor, Contractor will meet with successor contractor to initiate transfer of responsibilities, which transfer activities will be subject to protection of Contractor's proprietary information and intellectual property and limited to activities necessary to effectuate DHCS's intellectual property and sublicensing rights as contained in Exhibit D(S) of this Contract.
3. Contractor will update, with reasonable input from the successor contractor, and implement its Turnover Plan. The revised Turnover Plan will specify transition of capabilities, including milestones, timelines and key deliverables; details and schedule of licenses and sublicenses, as contained in Exhibit D(S), for access to all Intellectual Property licensed to DHCS in accordance with Exhibit D(S), including but not limited to content and tools, by DHCS and the successor contractor, to the extent such sublicense is permitted in accordance with Exhibit D(S); and, address specific details and timelines for exchange of user-data, including account and profile information, in accordance with Exhibit A, Attachment IV and the Business Associates Agreement and applicable laws.
4. Contractor will initiate formal Turnover and transfer of responsibilities in accordance with the DHCS-approved Turnover Plan.
5. Contractor will meet with successor contractor, and DHCS, at a frequency as detailed in the Contractor's DHCS-approved Turnover Plan.
6. Contractor will provide testing support to both DHCS and the successor contractor during Takeover testing under the successor contract.
7. Contractor will complete all requests for support, within a reasonable period, not to exceed ten (10) business days, unless DHCS provides written approval for a longer response period. This support will consist of, but is not limited to

the following, subject to protection of Contractor's proprietary information and intellectual property:

a) Submitting to DHCS, and/or the successor contractor, system files, test files, tables, and all other files and documentation needed to support parallel and other system testing.

b) Contractor Representative or his/her designee, certifying in writing that every item submitted is complete, current, and accurate and that the systems files, tables, and documentation in the submission are complete, current, and accurate copies of the files, tables, and documentation used in the production systems and operations. The certification will include a complete listing of all submitted items, along with a brief description of each.

c) Providing DHCS and successor contractor's staff with access to DHCS-owned or licensed electronic files and DHCS-licensed software, intellectual property, and equipment in Contractor's possession as needed to conduct testing, as necessary to effectuate DHCS's license and sublicensing rights in accordance with Exhibit D(S) of this Contract.

d) In no case will the granting of such access jeopardize Contractor's ability to meet Contract requirements. If Contractor's staff receives information that the actions of staff from the successor contractor may jeopardize operations, Contractor will advise DHCS, which will then advise Contractor whether to grant or deny access to successor contractor.

e) Assisting DHCS with the interpretation and analysis of test results.

f) Submitting any statistics requested by the DHCS relating to the accuracy of the information housed in operations.

g) Any other support requests from DHCS.

8. Contractor will submit to DHCS for review and written approval, which will not be withheld without cause, and for transfer to the successor Contractor, a detailed description of the methodology that will be utilized by the Contractor to ensure the complete review, certification, and acceptance of all operations documentation.

Exhibit A, Attachment II
Turnover Responsibilities

9. 12 months prior to LDO, and quarterly thereafter until LDO, submit to DHCS for review and written approval, which will not be withheld without cause, a comprehensive inventory list of all operations manuals and related documentation necessary for continued operations and to effectuate DHCS's intellectual property rights granted in Exhibit D(S). This inventory list will, at a minimum:
   a) Contain all operations manuals and related documentation identified in all areas of the Contract.
   b) Not contain copyrighted or proprietary information belonging to vendors and other entities.
   c) Be stored in DHCS approved information storage.
10. No later than twelve (12) months prior to LDO, and updated quarterly thereafter and at LDO, Contractor will submit a complete set of operations manuals, procedures, and related documentation necessary for continued operations and to effectuate DHCS's intellectual property rights granted in Exhibit D(S). Each submission will include the master list of operations manuals and related documentation. For each manual on the list, the Contractor will provide the manual title, a citation referencing the Contract section authorizing the creation of the manual, if applicable, and its current status (current, update pending, obsolete, etc.).
11. Continue to submit all documentation required to be submitted under the Contract, as required by DHCS, throughout Turnover. All such documents will be submitted in full compliance with the requirements set forth in the applicable Contract sections. The Contractor will ensure that these documents are added to the operations documentation to be submitted at LDO.
12. No later than one hundred and twenty (120) days prior to LDO, Contractor will submit to DHCS, for approval, a Turnover Communications Plan. The Communications Plan will, at a minimum, specify notification protocols and templates to notify users of the change of operations and transition to the successor contractor; transition of branding assets and marketing, as applicable and communication strategy, and messaging to notify stakeholders, as applicable.

Exhibit A, Attachment II
Turnover Responsibilities

E. Last Day of Operations (LDO) and Closeout

1. The Pre-LDO Phase and Turnover Closeout is defined as the last 4 months of operations under this Contract through 2 weeks prior to LDO.
2. During Pre-LDO, Contractor will:
    a) Prepare to complete its obligations under the terms of this Contract, and make all reasonable efforts to affect a smooth, problem-free turnover of Contract Operations to DHCS and the successor contractor.
    b) DHCS will provide the Contractor with the successor contractor's Assumption of Operations (AOO) Plan to assist with the development of the Turnover Phase-out Plan.
    c) 4 months prior to LDO, create a Turnover Phase-out Plan and submit to DHCS for review and approval. The Turnover Phase out Plan will identify all the activities through Turnover Closeout and the monitoring activities that will occur starting with LDO phase through Turnover closeout.
    d) Plan and implement pre-LDO, LDO, and post-LDO monitoring activities and reporting to DHCS.
    e) As reasonably directed by DHCS, meet with DHCS and/or the successor contractor to coordinate dependent activities through Pre-LDO and Turnover Closeout phases.
    f) Subject to obtaining an appropriate non-disclosure and confidentiality agreement from the successor contractor, the approved Turnover Phase-out Plan will be provided to the successor contractor to ensure the successor contractor coordinates dependent activities in the Assumption of Operations (AOO) Plan.
3. Turnover Closeout Plan and Schedule
4. The objective of the Turnover Closeout period is to plan and conduct activities that minimize the risk of disruption during the final turnover of operations.
5. 4 months prior to LDO, submit to DHCS for review and approval a Turnover Closeout Plan including a Closeout Transfer Schedule.
6. The Last Day of Operations (LDO) phase starts two (2) weeks prior to LDO and concludes 2 weeks after LDO. Contractor will transfer operations to the successor contractor so as to minimize the likelihood of disrupting the provision of services during the transfer process.

F. Transfer, as directed by DHCS, all associated operating manuals, maintenance agreements, and any and all documentation covering all operations activities as necessary to effectuate DHCS's licensing and sublicensing rights contained in Exhibit D(S).

Exhibit A, Attachment II
Turnover Responsibilities

G. In accordance with the Contract delivery requirements, complete all daily, weekly, and monthly reporting-in-process by the LDO, with delivery to the successor contractor on the following business day.

H. Submit, on or about LDO as approved by DHCS, all updates to information previously given to the successor contractor during the Turnover period.

I. The Post-LDO phase begins immediately after LDO and concludes 3 months after LDO, on the Contract Termination Date (CTD). Activities during this period include completion of transfers and deliverables and confirming all Operational and non-Operational components have been transferred to the successor Contractor.

J. Post-LDO Requirements

1. Complete transfer of all residual records to DHCS or the successor contractor.
2. Complete all other transfers, as applicable.
3. Monitor, track, and correct all issues identified during Post-LDO Phase. Issues must be logged in the Turnover Risk and Issue Tracking and Reporting System used during Turnover.
4. Notify DHCS within 12 hours of any issue materially and negatively impacting users.
5. Make available all key personnel to DHCS and the successor contractor to answer questions.
6. Turnover will be considered completed and the Contractor’s Turnover responsibilities accomplished upon the conclusion of the following items as approved in writing by DHCS:
    a) Completion of all plans and activities required in this section of the Contract.
    b) All Turnover deliverables and activities including, but not limited to, functions manuals, and artifacts.
    c) Transfer of all relevant user-data to DHCS and successor contractor, as permitted by law and applicable user consents.
    d) Correction, as reasonably achievable, to the reasonable satisfaction of DHCS, of all errors and/or deficiencies identified during Turnover.
    e) Receipt, and confirmation of readability, of all information files required by this Exhibit by the successor contractor.
    f) Submission of the final Turnover Issue and Risk log used through Turnover closeout.

Exhibit A, Attachment II
Turnover Responsibilities

g) Submission of the final version of the Turnover Work Plan.

h) Submission of Lessons Learned document for Turnover Phase. This document will include Turnover activities, methodologies that worked well and recommendations for improvements from the Contractor's perspective.