CALIFORNIA MENTAL HEALTH SERVICES AUTHORITY
PARTICIPATION AGREEMENT
COVER SHEET

1. Humboldt County ("Participant") desires to participate in the Program identified below.

   Name of Program: Interoperability Solution

   Summary of Program: CalMHSA will provide "CalMHSA Connex," a managed Interoperability Software as a Service (SaaS) solution (the "Services"), to assist participating counties in meeting state and federal interoperability requirements. CalMHSA Connex will facilitate the exchange of protected health information (PHI), personally identifiable information (PII) and other information between organizations and will assist Participants in connecting to larger national exchange networks.

2. California Mental Health Services Authority ("CalMHSA") and Participant acknowledge that the Program will be governed by CalMHSA's Joint Powers Agreement and its Bylaws, and by this participation agreement (the "Agreement"). The following exhibits are intended to clarify how the provisions of those documents will be applied to this Program.

   - þ Exhibit A Program Description and Funding
   - þ Exhibit B General Terms and Conditions
   - þ Exhibit C Data Sharing Agreement
   - þ Exhibit D Business Associate Agreement

3. The amount payable for the term of this Agreement is $222,948.

   This amount is comprised of a one-time Implementation and Project Management fee plus an annual Managed Services subscription fee. Additional fees may apply if Participant requests additional work or customizations not included in Exhibit A, Section III. Scope of Work, or where third-party fees are applicable.

4. The term of the Program is January 1, 2024, through December 31, 2026.

Authorized Signatures:

CalMHSA:

Signed: _____ Name (Printed): Dr. Amie Miller, Psy.D., MFT

Title: Executive Director Date: _____

Participant (Humboldt County):

Signed: _____ Name (Printed): Emi Botzler-Rodgers

Title: Behavioral Health Director Date: _____

Participation Agreement
EXHIBIT A – PROGRAM DESCRIPTION AND FUNDING

I. Name of Program: Interoperability Solution

II. Term of Program: January 1, 2024, through December 31, 2026.

III. Scope of Work:

CalMHSA will provide Participant the following services:

A. CalMHSA Responsibilities

1. California Data Exchange Framework ("DxF") Data Exchange Requirements.
    a. CalMHSA will provide a third-party brokered Integrating the Healthcare Enterprise (IHE) gateway and/or FHIR endpoint and workflow to facilitate query/response data exchange transactions via CalMHSA Connex. Available data exchange architecture(s) will align with industry standards and include the following options:
        i. Fast Healthcare Interoperability Resources (FHIR);
        ii. Cross-Community Access/Patient Discovery (XCA/XCPD);
        iii. Cross Enterprise Document Sharing (XDS.b).
    b. The Services will include a single bi-directional interface, which will include one inbound and one outbound connection to CalMHSA Connex.
    c. CalMHSA will assist Participant in producing necessary reporting and attestation to the Center for Data Insights and Innovation ("CDII") for organizations applying for DxF grant funding through CalMHSA as an umbrella applicant.
2. CMS Interoperability and Patient Access.
    a. CalMHSA will provide a technical solution to assist counties in complying with the following CMS Interoperability requirements:
        i. Patient Access API – CalMHSA will implement and maintain a secure, standards-based API (HL7 FHIR Release 4.0.1) that allows patients to access their claims and encounter information, as well as a defined sub-set of their clinical information, through third-party applications of their choice.
        ii. Provider Directory API – CalMHSA will make provider directory information publicly available via a standards-based API. CalMHSA will provide Participant with a Provider directory link to publish on Participant's County website.
        iii. Information Blocking regulations.
        iv. Receipt of Admission, Discharge, and Transfer (ADT) Event Notification.
            a) Receipt of ADTs is contingent on source organizations providing the requested data. CalMHSA will provide the means of processing and ingesting. Participant intervention may be needed to facilitate arrangements to receive appropriate messages. Third party fees may apply and will be paid by Participant.

3. CalMHSA will manage the implementation of interoperability services, including, but not limited to project management, set-up and configuration, and validation. Implementation professional services including:
    a. Developing data flow process for bi-directional data exchange.
    b. Overseeing implementation of county endpoints.
    c. Developing and implementing CMS interoperability requirements for Patient Access and Provider Directory, per CMS guidelines.
    d. Work to establish connection within Participant's EHR instance.
        i. CalMHSA will work to establish connection with Participant's instance within CalMHSA's SmartCare EHR program.
        ii. Connections to non-CalMHSA SmartCare EHR and non-SmartCare EHR systems will be addressed upon Participant's request.
        iii. Any such connections may require additional scope of work and may be subject to additional costs.
4. CalMHSA will manage operational availability of connections to include:
    a. Managing interoperability infrastructure.
    b. Monitoring security, HIPAA compliance and applicable data governance to the extent allowed by third party hosting service.
    c. Maintaining uptime of on-demand, real-time bi-directional data exchange process during the hours of 8:00am – 5:00pm PST, Monday through Friday. Uptime is subject to the terms as stated in Exhibit B, Section VI. Uptime and Support.
        i. Enabling XCA/XCPD endpoint, on behalf of County, for response to document queries for DxF compliance.
5. CalMHSA will provide training and support to Participant's staff regarding the Services.
    a. Training will be held remotely via webinar format.
    b. CalMHSA will make available recorded training videos for future reference.
6. CalMHSA will develop policies and procedures related to the Services and CalMHSA Connex.
    a. During interface implementation, CalMHSA will advise on interoperability best practices and assist county designated process owners and/or relevant staff with creating or modifying policies and procedures around interoperability.
7. Additional work or customizations requested by Participant outside of the Scope of Work included in this Agreement shall be subject to additional fees and must be agreed upon in a written contract signed by the Parties.

B. Participant Responsibilities

Participant shall be responsible for the following:

1. Data Delivery – Participant will deliver data to CalMHSA in a relational structured format. Participant agrees to take steps necessary to ensure data is extracted in the appropriate format including, but not limited to, working with their current vendor.

2. ISO Object Identifier (OID) - An OID is a globally unique ISO (International Organization for Standardization) identifier. An OID is required to facilitate on-demand, bi-directional data exchange. Participants are required to procure an OID.

3. Project Management and Coordination – Participant agrees to assign staff and a lead contact to communicate and collaborate with CalMHSA throughout the Interoperability project.

IV. Fee Structure

Service Type	One-Time Fee	Annual Rate
Implementation and Project Management	$100,000	
CalMHSA Managed Services Annual Subscription*		$39,000

*CalMHSA Managed Services Annual Subscription fee is subject to a five percent (5%) annual increase.

Participation Agreement
EXHIBIT B – General Terms and Conditions

I. Definitions

The following words, as used throughout this Participation Agreement, shall be construed to have the following meaning, unless otherwise apparent from the context in which they are used:

A. CalMHSA – California Mental Health Services Authority, a Joint Powers Authority (JPA) created by counties in 2009 at the instigation of the California Mental Health Directors Association to jointly develop and fund mental health services and education programs.

B. Member – A PARTICIPANT (or JPA of two or more Counties) that has joined CalMHSA and executed the CalMHSA Joint Powers Agreement.

C. Participant – Any County participating in the Program either as Member of CalMHSA or under a Memorandum of Understanding with CalMHSA.

D. Program – The program identified in the Cover Sheet.

II. Responsibilities

A. Responsibilities of CalMHSA:

1. Act as the Fiscal and Administrative agent for the Program.
2. Manage funds received consistent with the requirements of any applicable laws, regulations, guidelines and/or contractual obligations.
3. Provide regular fiscal reports to Participant and/or other public agencies with a right to such reports.
4. Comply with CalMHSA's Joint Powers Agreement and Bylaws.

B. Responsibilities of Participant:

1. Transfer of funding amount for the Program as specified in Exhibit B, Section V. Fiscal Provisions, which Participant will pay within the payment terms defined within this agreement.
2. Provide CalMHSA and any other parties deemed necessary with requested information and assistance to fulfill the purpose of the Program.
3. Any and all assessments, creation of individual case plans, and providing or arranging for services.
4. Provide CalMHSA with requested information and assistance to fulfill the purpose of the Program.
5. Provide feedback on Program performance.
6. Comply with applicable laws, regulations, guidelines, contractual agreements, JPAs, and bylaws.

III. Duration, Term, and Amendment

A. The term of the Program is January 1, 2024, through December 31, 2026.

B. This Agreement may be supplemented, amended, or modified only by the mutual agreement of CalMHSA and the Participant, expressed in writing and signed by authorized representatives of both parties.

IV. Withdrawal, Cancellation, and Termination

A. Participant may withdraw from the Program and terminate the Participation Agreement upon six (6) months' written notice. Notice shall be deemed served on the date of mailing.

B. The withdrawal of a Participant from the Program shall not automatically terminate its responsibility for its share of the expense and liabilities of the Program. The contributions of current and past Participants are chargeable for their respective share of unavoidable expenses and liabilities arising during the period of their participation.

V. Fiscal Provisions

A. Funding required from Participant shall be in the amount stated on the Cover Sheet of this Agreement.

B. Payment Terms – Participant will be invoiced annually by CalMHSA, and Participant will issue payment amount identified below within thirty (30) days of invoicing.

Payment for Year 1 will be due within thirty (30) days of execution of this Participation Agreement. Payment for Years 2 and 3 will be invoiced on and due within thirty (30) days of January 1 of the applicable fiscal period. See below.

Year	APPLICABLE FISCAL PERIOD	AMOUNT
1	1/1/2024 - 12/31/2024	$139,000
2	1/1/2025- 12/31/2025	$40,950
3	1/1/2026- 12/31/2026	$42,998

C. In a Multi-County Program, Participants will share the costs of planning, administration, and evaluation in the same proportions as their overall contributions, which are included in the amount stated in Exhibit A, Program Description and Funding.

VI. Uptime and Support

A. CalMHSA provides email support Monday through Friday, 8:00 a.m. to 5:00 p.m. PST. For any support questions please email: connex@calmhsa.org.

B. The services may occasionally become temporarily unavailable for maintenance purposes or other reasons outside of CalMHSA's control. CalMHSA will make best efforts to minimize any such unavailability.

VII. Disclaimer of Warranties

CALMHSA MAKES NO WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, GUARANTEES OR CONDITIONS WITH RESPECT TO THE PROGRAM. THESE DISCLAIMERS WILL APPLY EXCEPT TO THE EXTENT APPLICABLE LAW DOES NOT PERMIT THEM.

VIII. Limitation of Liability

THE AGGREGATE LIABILITY OF EACH PARTY FOR ALL CLAIMS UNDER THIS AGREEMENT IS LIMITED TO DIRECT DAMAGES UP TO THE AMOUNT PAID UNDER THIS AGREEMENT FOR THE PROGRAM DURING THE 12 MONTHS BEFORE THE CAUSE OF ACTION AROSE. NEITHER PARTY WILL BE LIABLE FOR LOSS OF REVENUE OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES, OR DAMAGES FOR LOST PROFITS, REVENUES, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION, EVEN IF THE PARTY KNEW THEY WERE POSSIBLE OR REASONABLY FORESEEABLE.

Participation Agreement
EXHIBIT C – DATA SHARING AGREEMENT

1. PARTIES

This Data Sharing Agreement ("DSA") is made by and between the parties to the underlying Participation Agreement (each individually a "Party" and collectively the "Parties") who are required to or elect to exchange Protected Health Information ("PHI"), Personally Identifiable Information ("PII") or other data in accordance with this Agreement, as defined below.

2. PURPOSE AND AUTHORITY

The privacy, security and integrity of PHI, PII and other data exchanged pursuant to this DSA and the underlying Participation Agreement are essential. This DSA is intended to facilitate data exchange between the Parties in compliance with all applicable federal, state, and local laws, regulations, and policies. This DSA sets forth a common set of terms, conditions, and obligations to support secure real-time access to, or exchange of, PHI, PII and other data between and among the Parties.

3. DEFINITIONS

A. "Agreement" shall mean this Data Sharing Agreement.

B. "Applicable Law" shall mean all federal, state, local, or tribal laws and regulations then in effect and applicable to the subject matter herein. For the avoidance of doubt, federal government entities are only subject to federal law.

C. "Authorization" shall have the meaning and include the requirements set forth at 45 CFR § 164.508 of the HIPAA Regulations and at Cal. Civ. Code § 56.05. The term shall include all requirements for obtaining consent to disclose confidential substance abuse disorder treatment records as set forth in 42 C.F.R. Part 2, when applicable, and shall include any additional requirements under Applicable Law to disclose PHI or PII.

D. "Breach" shall mean the unauthorized acquisition, access, disclosure, or use of PHI, PII or other data in a manner not permitted by the Agreement or Applicable Law.

E. "Business Associate" shall mean an organization that is defined as a "business associate" in 45 C.F.R. § 160.103 of the HIPAA Regulations.

F. "Confidential Participant Information" shall mean proprietary or confidential materials or information of a Party in any medium or format that a Party labels as such upon disclosure or that, given the nature of the information or the circumstances surrounding its disclosure, reasonably should be considered confidential. Notwithstanding any label to the contrary, Confidential Participant Information does not include any information which is or becomes

known publicly through no fault of the party to which such information is disclosed (a "Receiving Party"); is learned of by a Receiving Party from a third party entitled to disclose it; is already known to a Receiving Party before receipt from the disclosing Party as documented by the Receiving Party's written records; or is independently developed by a Receiving Party without reference to, reliance on, or use of the disclosing Party's Confidential Participant Information.

G. "Covered Entity" shall have the meaning set forth at 45 C.F.R. § 160.103 and shall also include the following as these terms are defined in California Civil Code § 56.05: "provider of health care," "health care service plan," and "licensed health care professional."

H. "Effective Date" shall mean the date of execution of the underlying Participation Agreement.

I. "Governmental Participants" shall mean those Parties that are local (e.g., municipalities, counties), state, tribal, or federal entities.

J. "Health Care Operations" for the purposes of this Agreement shall consist of the following activities:

I. Quality Assessment and Improvement activities as described in subsection (1) of the definition of health care operations set forth at 45 C.F.R. § 164.501.

II. Population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination and contacting of health care providers and patients with information about treatment alternatives as set forth at 45 C.F.R. § 154.501.

K. "HIPAA Regulations" shall mean the standards for privacy of individually identifiable health information, the security standards for the protection of electronic protected health information and the breach notification rule (45 C.F.R. §§ 160 and 164) promulgated by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as in effect on the Effective Date and as may be amended, modified, or renumbered.

L. "Individual User" shall mean the person who is the subject of PHI or PII.

M. "Payment" shall have the same meaning as set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.

N. "Personally Identifiable Information" or "PII" shall have the same meaning as "Personal Information" set forth in Section 1798.140(o) of the California Civil Code, but shall be limited to PII exchanged pursuant to this Agreement.

O. “Personal Representative” shall refer to a person who, under Applicable Law, has authority to act on behalf of an individual as set forth in 45 C.F.R. § 164.502(g).

P. “Protected Health Information” or “PHI” shall refer to “protected health information” as set forth at 45 C.F.R. § 160.103 of the HIPAA Regulations and “medical information” as set forth at Civil Code § 56.05.

Q. “Public Health Activities” shall mean an access, use or disclosure permitted under the HIPAA Regulations and any other Applicable Law for public health activities and purposes, including an access, use or disclosure permitted under 45 C.F.R. § 164.512(b) and 45 C.F.R. § 164.514(e). Public Health Activities excludes the following oversight activities: audits; civil, administrative or criminal investigations; inspections; licensure or disciplinary actions; and civil, administrative or criminal proceedings or actions other than enforcement activities by a county health officer that are authorized under Cal. Health & Safety Code § 101030.

R. “Health Information Exchange” or “HIE” shall mean a data exchange intermediary that facilitates the exchange of patient information or other data.

S. “Recipient” shall mean a Party that receives PHI, PII or other data from a Submitter. For purposes of illustration only, Recipients include, but are not limited to, Parties who receive queries, responses, subscriptions, publications or unsolicited messages.

T. “Research” shall mean a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.

U. “Sale of Information” shall mean the disclosure of PHI, PII and/or other data in return for direct or indirect remuneration from or on behalf of the recipient of the Information. Sale of PHI, PII or other data shall not include the disclosure of PHI, PII or other data for the activities set forth in 45 C.F.R. § 164.502(a)(5)(ii)(B)(2).

V. “Social Services” shall mean the delivery of items, resources, and/or services to address social determinants of health and social drivers of health, including but not limited to housing, foster care, nutrition, access to food, transportation, employment, and other social needs.

W. “Social Services Activities” shall mean the Social Services provided by Social Service Organizations.

X. “Social Services Organization” shall mean a person or entity whose primary business purpose is to provide Social Services to individuals. Social Services Organizations can include but are not

limited to government entities (including multi-department health and human services agencies), community-based organizations, nonprofits, and private entities.

Y. "Submitter" shall mean a Party that submits PHI, PII or other data to a Recipient.

Z. "System" shall mean software, portal, platform, or other electronic medium controlled by a Party through which the Party conducts PHI, PII or other data exchange-related activities. For purposes of this definition, it shall not matter whether the Party controls the software, portal, platform, or medium through ownership, lease, license, or otherwise.

AA. "Treatment" shall have the same meaning as set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.

4. USE OF PHI, PII AND OTHER DATA

A. REQUIRED PURPOSES. Subject to applicable law, the Parties are required to exchange PHI, PII and other data and/or provide access to PHI, PII and other data pursuant to state and federal laws and regulations for Treatment, Payment, Health Care Operations and Public Health Activities as those terms are defined herein. Notwithstanding the foregoing, a Party may only disclose PHI, PII or other data to another Party for Health Care Operations if each entity either has or had a relationship with the Individual User who is the subject of the PHI, PII or data being requested and the PHI, PII or data pertains to such relationship.

B. PERMITTED PURPOSES. The Parties are permitted to exchange or provide access to PHI, PII and other data including information subject to 42 C.F.R. Part 2, for any purpose not set forth in Section C below, provided appropriate Authorizations are made, if necessary, and the disclosure or use of the PHI, PII or other data is permissible under Applicable Law.

C. PROHIBITED PURPOSES. Unless otherwise permitted by Applicable Law or a legally valid agreement, the Parties shall not access PHI, PII or other data related to this Agreement or the underlying Participation Agreement in order to sell such information. No Party shall access PHI, PII or other data related to this Agreement or the underlying Participation Agreement in order to unlawfully discriminate or unlawfully deny or limit access to medical services, or to prosecute or take any other adverse action against an individual who accesses medical services.

5. AUTHORIZATIONS

To the extent required by Applicable Law, the Parties shall not disclose PHI, PII or other data to another Party unless a legally valid Authorization has been obtained. For the avoidance of doubt, the Parties shall not be required to obtain an Authorization prior to disclosing PHI, PII or other data pursuant to this

Agreement unless an Authorization is required under Applicable Law. Any disclosure of PHI, PII or other data by a Submitter shall be deemed an express representation that the Submitter has complied with this Section and unless the Recipient has actual knowledge to the contrary, the Recipient may reasonably and justifiably rely upon such representation.

6. BREACH NOTIFICATION

A. OBLIGATIONS OF PARTIES.

I. As soon as reasonably practicable after discovering a Breach has occurred, and within any timeframes prescribed by an applicable Business Associate Agreement or required by Applicable Law, the discovering Party shall notify the Covered Entity and/or Party impacted by the breach of any confirmed or reasonably suspected Breach.

II. As soon as reasonably practicable after discovering a Breach has occurred, and within any timeframes prescribed by an applicable Business Associate Agreement or required by Applicable Law, the discovering Party shall provide a written report of the Breach to the Covered Entity and/or Party impacted by the Breach. The discovering Party shall supplement the information contained in the written report as it becomes available and shall cooperate with the Covered Entity and/or the Party impacted by the breach. The written report should include sufficient information for the recipient of the notification to understand the nature of the Breach. For instance, such written report should include, to the extent available, the following information:

a. A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident, or Breach and the date of Discovery of the non-permitted Use or Disclosure, Security Incident, or Breach, if known;

b. The number of Individuals whose PHI, PII or other data is involved;

c. A description of the specific type of PHI, PII or other data involved in the non-permitted Use or Disclosure, Security Incident, or Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

d. The identification of each Individual whose Unsecured PHI or PII has been, or is reasonably believed by the discovering Party to have been, accessed, acquired, Used, or Disclosed;

e. Any other information necessary to conduct an assessment of whether notification to the Individual(s) is required by applicable law;

f. Any steps the discovering Party believes that the Individual(s) could take to protect him or herself from potential harm from the non-permitted Use or Disclosure, Security Incident, or Breach;

g. A brief description of what the discovering Party is doing to investigate, to mitigate harm to the Individual(s), and to protect against any further similar occurrences; and

h. The name and contact information for a person highly knowledge of the facts and circumstances of the non-permitted Use or Disclosure of PHI, PII or other data, Security Incident, or Breach.

III. Notwithstanding the above, if a Party is notified, in writing or by oral statement by any law enforcement official or by any other governmental agency (e.g., Federal Trade Commission), that a Breach notification would impede a criminal investigation or cause damage to national security, and the statement has been documented consistent with 45 C.F.R. § 164.412(b), then the Party shall delay the Breach notification for the time period specified by the law enforcement official and as required by Applicable Law.

IV. Where conflict exists between the terms of this DSA and an applicable Business Associate Agreement, the Business Associate Agreement shall prevail.

7. PRIVACY AND SECURITY

A. GENERAL. The Parties agree to at all times fully comply with any applicable Business Associate Agreement and all applicable law relating to this Agreement and the use of PHI, PII and other data including, but not limited to, the HIPAA Regulations.

B. SAFEGUARDS. The Parties shall be responsible for maintaining a secure environment that supports the exchange of PHI, PII and other data as set forth in this Agreement and applicable law. Each Party, regardless of whether it, pursuant to federal law, is subject to the HIPAA Regulations, shall use appropriate safeguards to prevent unauthorized use or disclosure of PHI, PII and other data in a manner consistent with HIPAA Regulations, including implementing appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of PHI, PII and other data.

C. PRIVACY STANDARDS AND SAFEGUARDS RELATED TO BEHAVIORAL HEALTH. In the event that a Party uses, accesses, or discloses behavioral health information, the Party shall, prior to engaging in any such activity, implement appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of such information in accordance with Applicable Law, including but not limited to, 42 C.F.R. Part 2 and the California Lanterman-Petris-Short Act.

D. TRAINING POLICIES AND PROCEDURES. Each Party shall, pursuant to this Agreement, an applicable Business Associate Agreement, Applicable Law, or applicable federal and state guidance, have written privacy and security policies relating to the use and disclosure of PHI, PII and/or other data that are consistent with and satisfy the requirements set forth in the HIPAA Regulations and Applicable Law. Before granting access to PHI or PII, each Party shall train staff, contractors, agents, employees, and workforce members, as defined under the HIPAA Regulations, who will have access to PHI or PII under this Agreement. Each Party shall also provide refresher training consistent with each Party's internal privacy and security policies but no less than annually.

8. MINIMUM NECESSARY

Any use or disclosure of PHI or PII pursuant to this Agreement or the underlying Participation Agreement will be limited to the minimum PHI or PII necessary to achieve the purpose for which the information is shared, except where limiting such use or disclosure to the minimum necessary (i) is not feasible, (ii) is not required under the HIPAA Regulations (such as for Treatment) or any other Applicable Law, (iii) is a disclosure to an Individual User or Individual User's Personal Representative, (iv) is a disclosure pursuant to an Individual User's Authorization, or (v) is a disclosure required by Applicable Law.

9. INDIVIDUAL ACCESS

An Individual User or an Individual User's Personal Representative shall have the right to inspect, obtain a copy of, and have bidirectional electronic access to PHI or PII about the Individual User to the extent consistent with Applicable Law.

Prior to initiating Individual Access services, the Party shall be required to verify the identity of the Individual User or the Individual User's Personal Representative using standards and methods consistent with HIPAA regulations or other Applicable Law.

10. INDIVIDUAL USER OPT OUT

Nothing in this Agreement shall prohibit an Individual User or an Individual User's Personal Representative from opting out of having the Individual User's PHI or PII exchanged pursuant to this Agreement.

11. REASONABLE AND GOOD FAITH COOPERATION

The Parties to this Agreement agree to cooperate in good to implement the provisions of this Agreement. The Parties agree to provide such non-privileged information to the reasonably requested for purposes of performing activities related to this Agreement and the underlying Participation Agreement. The Parties agree to provide any requested information and assistance to the other Party in the investigation of breaches and disputes, subject to the assisting Party's right to restrict or condition its cooperation or disclosure of information in the interest of (A) preserving privileges in any foreseeable dispute or litigation or (B) protecting its Confidential Participant Information. In no case shall a Party be required to disclose PHI or PII in violation of Applicable Law.

12. COMPLIANCE WITH THIS AGREEMENT

Except to the extent prohibited by Applicable Law, each Party shall comply fully with all provisions of this Agreement. To the extent that a Party delegates its duties under this Agreement to a third party (by contract or otherwise) and such third party will have access to PHI, PII or other data pursuant to this Agreement, that delegation shall be in writing and require the third party, prior to exchanging PHI, PII or other data, to agree to the same restrictions and conditions that apply through this Agreement to the Parties.

13. ACCURACY OF PHI, PII AND OTHER DATA

When acting as a Submitter, each Party represents that at the time of transmission, the PHI, PII and/or other data it provides is an accurate representation of the data contained in, or available through, its System and is (i) sent from a System that employs security controls that meet industry standards so that the PHI, PII and/or other data being transmitted is intended to be free from malicious software, and (ii) provided in a timely manner.

14. EXPRESS WARRANTY OF AUTHORITY TO EXCHANGE INFORMATION

To the extent each Party discloses PHI, PII or other data to the other Party, the disclosing Party represents and warrants that it has sufficient authority to disclose such PHI, PII and/or other data.

15. THIRD-PARTY TECHNOLOGY

The Parties acknowledge that each Party may use technology solutions, applications, interfaces, software, platforms, clearinghouses, and other IT resources to support exchange of PHI, PII and other data that may be provided by third parties ("Third-Party Technology"). Each Party shall have agreements in place that require Third-Party Technology vendors (i) to provide reliable, stable, and secure services to the Party and (ii) to adhere to the same or similar privacy and security standards applicable to the Party pursuant to this Agreement. However, each Party acknowledges that Third-Party Technology may be interrupted or not available at times and that this could prevent a Party from transmitting PHI, PII or other data. The Parties do not make any representations or warranties as to their Third-Party

Technology.

16. TERM

This Agreement shall commence on the Effective Date of the underlying agreement and shall continue until termination or expiration of the underlying agreement.

17. EFFECT OF TERMINATION

Upon any termination of this Agreement for any reason the Parties shall have no rights under this Agreement to exchange data with each other. Termination of this Agreement shall not affect any rights or obligations which by their terms should survive termination or expiration.

18. LIABILITY

Each Party shall be responsible for its acts and omissions and not for the acts or omissions of the other Party. Notwithstanding any provision in this Agreement to the contrary, neither Party shall be liable for any act or omission if a cause of action for such act or omission is otherwise prohibited by Applicable Law.

19. GOVERNING LAW

This Agreement shall be governed and enforced pursuant to the laws of the State of California, without giving effect to its conflicts of laws provisions, except to the extent California law is preempted by any provision of federal law.

20. ASSIGNMENT

Neither Party shall assign or transfer this Agreement, or any part thereof, without the express written consent of the other Party, which shall not be unreasonably delayed or denied. Any assignment that does not comply with the requirements of this Section shall be void and have no binding effect.

21. SURVIVAL

All Sections which by their nature are meant to survive this Agreement shall survive expiration or termination of this Agreement.

22. WAIVER

No failure or delay by any Party in exercising its rights under this Agreement shall operate as a waiver of such rights, and no waiver of any right shall constitute a waiver of any prior, concurrent, or subsequent right.

23. THIRD-PARTY BENEFICIARIES

Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

24. FORCE MAJEUR

No Party shall be responsible for any delays or failures in performance caused by the occurrence of events or other circumstances that are beyond its reasonable control after the exercise of commercially reasonable efforts to either prevent or mitigate the effect of any such occurrence or event.

Participation Agreement
EXHIBIT D – BUSINESS ASSOCIATE AGREEMENT

See Attached County Signed Business Associate Agreement

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

Agreement No.: 1733-BAA-2022-HC
Humboldt County
September 21, 2022

BUSINESS ASSOCIATE AGREEMENT
UNDER THE HEALTH INSURANCE PORTABILITY
AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

Humboldt County ("County"), a member of the California Mental Health Services Authority ("CalMHSA") Joint Powers Authority ("JPA"), is a Covered Entity as defined by, and subject to the requirements and prohibitions of, the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), and regulations promulgated thereunder, including the Privacy, Security, Breach Notification, and Enforcement Rules at 45 Code of Federal Regulations (C.F.R.) Parts 160 and 164 (collectively, the "HIPAA Rules").

Pursuant to the JPA Agreement, CalMHSA, hereinafter referred to as "Contractor", performs or provides functions, activities or services to County that require Contractor to create, access, receive, maintain, and/or transmit information that includes or that may include Protected Health Information, as defined by the HIPAA Rules in order to provide such functions, activities or services. As such, Contractor is a Business Associate, as defined by the HIPAA Rules, and is therefore subject to those provisions of the HIPAA Rules that are applicable to Business Associates.

The HIPAA Rules require a written agreement ("Business Associate Agreement") between County and Contractor in order to mandate certain protections for the privacy and security of Protected Health Information, and these HIPAA Rules prohibit the disclosure to or use of Protected Health Information by Contractor if such an agreement is not in place. In addition, the California Department of Health Care Services ("DHCS") requires County and Contractor to include certain protections for the privacy and security of personal information ("PI"), sensitive information, and confidential information (collectively, "PSCI"), personally identifiable information ("PII") not subject to HIPAA ("DHCS Requirements").

This Business Associate Agreement and its provisions are intended to protect the privacy and provide for the security of Protected Health Information, PSCI, and PII disclosed to or used by Contractor in compliance with the HIPAA Rules and DHCS Requirements.

Therefore, the parties agree as follows:

1. DEFINITIONS

1.1 "Breach" has the same meaning as the term "breach" at 45 C.F.R. § 164.402.

1.2 "Breach Notification Rule" shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and D.

1.3 "Business Associate" has the same meaning as the term "business associate" at 45 C.F.R. § 160.103. For the convenience of the parties, a "business associate" is a person or entity, other than a member of the workforce of covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to Protected Health Information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of another business associate. And in reference to the party to this Business Associate Agreement "Business Associate" shall mean Contractor.

1.4 "California Confidentiality Laws" means the applicable laws of the State of California governing the confidentiality, privacy, or security of PHI or other PII, including, but not limited to, the California Confidentiality of Medical Information Act (Cal. Civil Code § 56 et seq.), the patient

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

access law (Cal. Health & Safety Code § 123100 et seq.), the HIV test result confidentiality law (Cal. Health & Safety Code § 120975 et seq.), the Lanterman-Petris-Short Act (Cal. Welf. & Inst. Code § 5328 et seq.), and California's data breach law (Cal. Civil Code § 1798.29).

1.5 "Covered Entity" has the same meaning as the term "covered entity" at 45 C.F.R. § 160.103, and in reference to the party to this Business Associate Agreement, "Covered Entity" shall mean County.

1.6 "Data Aggregation" has the same meaning as the term "data aggregation" at 45 C.F.R. § 164.501.

1.7 "De-identification" refers to the de-identification standard at 45 C.F.R. § 164.514.

1.8 "Designated Record Set" has the same meaning as the term "designated record set" at 45

1.9 C.F.R. § 164.501."Disclose" and "Disclosure" mean, with respect to Protected Health Information, the release, transfer, provision of access to, or divulging in any other manner of Protected Health Information outside Business Associate's internal operations or to other than its workforce. (See 45 C.F.R. § 160.103.)

1.10 "Electronic Health Record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. (See 42 U.S. C. § 17921.)

1.11 "Electronic Media" has the same meaning as the term "electronic media" at 45 C.F.R. § 160.103. For the convenience of the parties, electronic media means (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

1.12 "Electronic Protected Health Information" has the same meaning as the term "electronic protected health information" at 45 C.F.R. § 160.103, limited to Protected Health Information created or received by Business Associate from or on behalf of Covered Entity. For the convenience of the parties, Electronic Protected Health Information means Protected Health Information that is (i) transmitted by electronic media; (ii) maintained in electronic media.

1.13 "Health Care Operations" has the same meaning as the term "health care operations" at 45 C.F.R. § 164.501.

1.14 "Individual" has the same meaning as the term "individual" at 45 C.F.R. § 160.103. For the convenience of the parties, Individual means the person who is the subject of Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502 (g).

1.15 "Law Enforcement Official" has the same meaning as the term "law enforcement official" at 45 C.F.R. § 164.103.

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

1.16 "Minimum Necessary" refers to the minimum necessary standard at 45 C.F.R. § 162.502(b).

1.17 “Protected Health Information” has the same meaning as the term “protected health information” at 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity. For the convenience of the parties, Protected Health Information includes information that (i) relates to the past, present or future physical or mental health or condition of an Individual; the provision of health care to an Individual, or the past, present or future payment for the provision of health care to an Individual; (ii) identifies the Individual (or for which there is a reasonable basis for believing that the information can be used to identify the Individual); and (iii) is created, received, maintained, or transmitted by Business Associate from or on behalf of Covered Entity, and includes Protected Health Information that is made accessible to Business Associate by Covered Entity. “Protected Health Information” includes Electronic Protected Health Information.

1.18 “Required by Law” " has the same meaning as the term "required by law" at 45 C.F.R. § 164.103.

1.19 "Secretary" has the same meaning as the term "secretary" at 45 C.F.R. § 160.103

1.20 "Security Incident” has the same meaning as the term "security incident" at 45 C.F.R. § 164.304.

1.20 "Services” means, unless otherwise specified, those functions, activities, or services in the applicable underlying Agreement, Contract, Master Agreement, Work Order, or Purchase Order or other service arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

1.21 "Subcontractor" has the same meaning as the term "subcontractor" at 45 C.F.R. § 160.103.

1.22 "Unsecured Protected Health Information" has the same meaning as the term “unsecured protected health information" at 45 C.F.R. § 164.402.

1.23 “Use” or “Uses” means, with respect to Protected Health Information, the sharing, employment, application, utilization, examination or analysis of such Information within Business Associate’s internal operations. (See 45 C.F.R § 164.103.)

1.24 Terms used, but not otherwise defined in this Business Associate Agreement, have the same meaning as those terms in the HIPAA Rules.

2. PERMITTED AND REQUIRED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

2.1 Business Associate may only Use and/or Disclose Protected Health Information as necessary to perform Services, and/or as necessary to comply with the obligations of this Business Associate Agreement.

2.2 Business Associate may Use Protected Health Information for de-identification of the information if de-identification of the information is required to provide Services.

2.3 Business Associate may Use or Disclose Protected Health Information as Required by Law.

2.4 Business Associate shall make Uses and Disclosures and requests for Protected Health Information consistent with the Covered Entity’s applicable Minimum Necessary policies and

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

procedures.

2.5 Business Associate may Use Protected Health Information as necessary for the proper management and administration of its business or to carry out its legal responsibilities.

2.6 Business Associate may Disclose Protected Health Information as necessary for the proper management and administration of its business or to carry out its legal responsibilities, provided the Disclosure is Required by Law or Business Associate obtains reasonable assurances from the person to whom the Protected Health Information is disclosed (i.e., the recipient) that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purposes for which it was disclosed to the recipient and the recipient notifies Business Associate of any instances of which it is aware in which the confidentiality of the Protected Health Information has been breached.

2.7 Business Associate may provide Data Aggregation services relating to Covered Entity's Health Care Operations if such Data Aggregation services are necessary in order to provide Services.

3. PROHIBITED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

3.1 Business Associate shall not Use or Disclose Protected Health Information other than as permitted or required by this Business Associate Agreement or as Required by Law.

3.2 Business Associate shall not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164, or the California Confidentiality Laws if done by Covered Entity, except for the specific Uses and Disclosures set forth in Sections 2.5 and 2.6.

3.3 Business Associate shall not Use or Disclose Protected Health Information for de- identification of the information except as set forth in section 2.2.

4. OBLIGATIONS TO SAFEGUARD PROTECTED HEALTH INFORMATION

4.1 Business Associate shall implement, use, and maintain appropriate safeguards to prevent the Use or Disclosure of Protected Health Information other than as provided for by this Business Associate Agreement.

4.2 Business Associate shall comply with Subpart C of 45 C.F.R Part 164 with respect to Electronic Protected Health Information, to prevent the Use or Disclosure of such information other than as provided for by this Business Associate Agreement.

5. REPORTING NON-PERMITTED USES OR DISCLOSURES, SECURITY INCIDENTS, AND BREACHES OF UNSECURED PROTECTED HEALTH INFORMATION

5.1 Business Associate shall report to Covered Entity any Use or Disclosure of Protected Health Information not permitted by this Business Associate Agreement, any Security Incident, and/ or any Breach of Unsecured Protected Health Information as further described in Sections 5.1.1, 5.1.2, and 5.1.3.

5.1.1 Business Associate shall report to Covered Entity any Use or Disclosure of Protected Health Information by Business Associate, its employees, representatives, agents or

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

Subcontractors not provided for by this Agreement of which Business Associate becomes aware.

5.1.2 Business Associate shall report to Covered Entity any Security Incident of which Business Associate becomes aware.

5.1.3 Business Associate shall report to Covered Entity any Breach by Business Associate, its employees, representatives, agents, workforce members, or Subcontractors of Unsecured Protected Health Information that is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate. Business Associate shall be deemed to have knowledge of a Breach of Unsecured Protected Health Information if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of Business Associate, including a Subcontractor, as determined in accordance with the federal common law of agency.

5.2 Except as provided in Section 5.3, for any reporting required by Section 5.1, Business Associate shall provide, to the extent available, all information required by, and within the times frames specified in, Sections 5.2.1 and 5.2.2.

5.2.1 Business Associate shall make an immediate telephonic report upon discovery of the non-permitted Use or Disclosure of Protected Health Information, Security Incident or Breach of Unsecured Protected Health Information to **County of Humboldt, DHHS Compliance Line 707-441-5410 or Toll Free 833-691-1200** that minimally includes:

(a) A brief description of what happened, including the date of the non- permitted Use or Disclosure, Security Incident, or Breach and the date of Discovery of the non-permitted Use or Disclosure, Security Incident, or Breach, if known;

(b) The number of Individuals whose Protected Health Information is involved;

(c) A description of the specific type of Protected Health Information involved in the non-permitted Use or Disclosure, Security Incident, or Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

(d) The name and contact information for a person highly knowledge of the facts and circumstances of the non-permitted Use or Disclosure of PHI, Security Incident, or Breach.

5.2.2 Business Associate shall make a written report without unreasonable delay and in no event later than three (3) business days from the date of discovery by Business Associate of the non-permitted Use or Disclosure of Protected Health Information, Security Incident, or Breach of Unsecured Protected Health Information and to the

Chief Security Officer: Zach Smith
County, Department: Humboldt County, Department of Health and Human Services (DHHS),

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

Address__507 F. Street, Eureka CA 95501 _____,
Email___ _____ zsmith@co.humboldt.ca.us _____,

and,

Name: _Amy Cone_____
County, Department:_Humboldt County, Department of Health and Human Services (DHHS),
Address:__507 F. Street, Eureka CA 95501_____,
Email___acone@co.humboldt.ca.us _____,

that includes, to the extent possible:

(a) A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident, or Breach and the date of Discovery of the non-permitted Use or Disclosure, Security Incident, or Breach, if known;

(b) The number of Individuals whose Protected Health Information is involved;

(c) A description of the specific type of Protected Health Information involved in the non-permitted Use or Disclosure, Security Incident, or Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

(d) The identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, Used, or Disclosed;

(e) Any other information necessary to conduct an assessment of whether notification to the Individual(s) under 45 C.F.R. § 164.404 is required;

(f) Any steps Business Associate believes that the Individual(s) could take to protect him or herself from potential harm from the non-permitted Use or Disclosure, Security Incident, or Breach;

(g) A brief description of what Business Associate is doing to investigate, to mitigate harm to the Individual(s), and to protect against any further similar occurrences; and

(h) The name and contact information for a person highly knowledge of the facts and circumstances of the non-permitted Use or Disclosure of PHI, Security Incident, or Breach.

5.2.3 If Business Associate is not able to provide the information specified in Section 5.2.1 or 5.2.2 at the time of the required report, Business Associate shall provide such information promptly thereafter as such information becomes available.

5.3 Business Associate may delay the notification required by Section 5.1.3, if a verified law enforcement official states to Business Associate that notification would impede a criminal investigation or cause damage to national security.

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

5.3.1 If the law enforcement official's statement is in writing and specifies the time for which a delay is required, Business Associate shall delay its reporting and/or notification obligation(s) for the time period specified by the official.

5.3.2 If the statement is made orally, Business Associate shall document the statement, including the identity of the official making the statement, and delay its reporting and/or notification obligation(s) temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in Section 5.3.1 is submitted during that time.

6. WRITTEN ASSURANCES OF SUBCONTRACTORS

6.1 In accordance with 45 C.F.R. § 164.502 (e)(1)(ii) and § 164.308 (b)(2), if applicable, Business Associate shall ensure that any Subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of Business Associate is made aware of its status as a Business Associate with respect to such information and that Subcontractor agrees in writing to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information.

6.2 Business Associate shall take reasonable steps to cure any material breach or violation by Subcontractor of the agreement required by Section 6.1.

6.3 If the steps required by Section 6.2 do not cure the breach or end the violation, Contractor shall terminate, if feasible, any arrangement with Subcontractor by which Subcontractor creates, receives, maintains, or transmits Protected Health Information on behalf of Business Associate.

6.4 If neither cure nor termination as set forth in Sections 6.2 and 6.3 is feasible, Business Associate shall immediately notify CalMHSA.

6.5 Without limiting the requirements of Section 6.1, the agreement required by Section 6.1 (Subcontractor Business Associate Agreement) shall require Subcontractor to contemporaneously notify Covered Entity in the event of a Breach of Unsecured Protected Health Information.

6.6 Without limiting the requirements of Section 6.1, agreement required by Section 6.1 (Subcontractor Business Associate Agreement) shall include a provision requiring Subcontractor to destroy, or in the alternative to return to Business Associate, any Protected Health Information created, received, maintained, or transmitted by Subcontractor on behalf of Business Associate so as to enable Business Associate to comply with the provisions of Section 18.4.

6.7 Business Associate shall provide to Covered Entity, at Covered Entity's request, a copy of any and all Subcontractor Business Associate Agreements required by Section 6.1.

6.8 Sections 6.1 and 6.7 are not intended by the parties to limit in any way the scope of Business Associate's obligations related to Subcontracts or Subcontracting in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

7. ACCESS TO PROTECTED HEALTH INFORMATION

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

7.1 To the extent Covered Entity determines that Protected Health Information is maintained by Business Associate or its agents or Subcontractors in a Designated Record Set, Business Associate shall, within two (2) business days after receipt of a request from Covered Entity, make the Protected Health Information specified by Covered Entity available to the Individual(s) identified by Covered Entity as being entitled to access and shall provide such Individuals(s) or other person(s) designated by Covered Entity with a copy the specified Protected Health Information, in order for Covered Entity to meet the requirements of 45 C.F.R. § 164.524 or the California Confidentiality Laws.

7.2 If any Individual requests access to Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within two (2) days of the receipt of the request. Whether access shall be provided or denied shall be determined by Covered Entity.

7.3 To the extent that Business Associate maintains Protected Health Information that is subject to access as set forth above in one or more Designated Record Sets electronically and if the Individual requests an electronic copy of such information, Business Associate shall provide the Individual with access to the Protected Health Information in the electronic form and format requested by the Individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by Covered Entity and the Individual.

8. AMENDMENT OF PROTECTED HEALTH INFORMATION

8.1 To the extent Covered Entity determines that any Protected Health Information is maintained by Business Associate or its agents or Subcontractors in a Designated Record Set, Business Associate shall, within ten (10) business days after receipt of a written request from Covered Entity, make any amendments to such Protected Health Information that are requested by Covered Entity, in order for Covered Entity to meet the requirements of 45 C.F.R. § 164.526.

8.2 If any Individual requests an amendment to Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of the receipt of the request. Whether an amendment shall be granted or denied shall be determined by Covered Entity.

9. ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

9.1 Business Associate shall maintain an accounting of each Disclosure of Protected Health Information made by Business Associate or its employees, agents, representatives or Subcontractors, as is determined by Covered Entity to be necessary in order to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.

9.1.1 Any accounting of disclosures provided by Business Associate under Section 9.1 shall include:

(a) The date of the Disclosure;

(b) The name, and address if known, of the entity or person who received the Protected Health Information;

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

(c) A brief description of the Protected Health Information Disclosed; and

(d) A brief statement of the purpose of the Disclosure.

9.1.2 For each Disclosure that could require an accounting under Section 9.1, Business Associate shall document the information specified in Section 9.1.1, and shall maintain the information for six (6) years from the date of the Disclosure.

9.2 Business Associate shall provide to Covered Entity, within ten (10) business days after receipt of a written request from Covered Entity, information collected in accordance with Section 9.1.1 to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528

9.3 If any Individual requests an accounting of disclosures directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of the receipt of the request, and shall provide the requested accounting of disclosures to the Individual(s) within 30 days. The information provided in the accounting shall be in accordance with 45 C.F.R. § 164.528.

10. COMPLIANCE WITH APPLICABLE FEDERAL AND STATE PRIVACY AND SECURITY RULES

10.1 To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, Business Associate shall comply with the requirements of Subpart E that apply to Covered Entity's performance of such obligation(s).

10.2 Business Associate shall comply with all HIPAA Rules and California Confidentiality Laws applicable to Business Associate in the performance of Services.

11. AVAILABILITY OF RECORDS

11.1 Business Associate shall make its internal practices, books, and records relating to the Use and Disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity available to the Secretary for purposes of determining Covered Entity's compliance with the Privacy and Security Regulations.

11.2 Unless prohibited by the Secretary, Business Associate shall immediately notify Covered Entity of any requests made by the Secretary and provide Covered Entity with copies of any documents produced in response to such request.

12. MITIGATION OF HARMFUL EFFECTS

12.1 Business Associate shall mitigate, to the extent practicable, any harmful effect of a Use or Disclosure of Protected Health Information by Business Associate in violation of the requirements of this Business Associate Agreement that is known to Business Associate.

13. BREACH NOTIFICATION TO INDIVIDUALS

13.1 Business Associate shall, to the extent Covered Entity determines that there has been a Breach of Unsecured Protected Health Information by Business Associate, its employees, representatives, agents or Subcontractors, provide breach notification to the Individual in a manner that permits Covered Entity to comply with its obligations under 45 C.F.R. § 164.404.

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

13.1.1 Business Associate shall notify, subject to the review and approval of Covered Entity, each Individual whose Unsecured Protected Health Information has been, or is reasonably believed to have been, accessed, acquired, Used, or Disclosed as a result of any such Breach.

13.1.2 The notification provided by Business Associate shall be written in plain language, shall be subject to review and approval by Covered Entity, and shall include, to the extent possible:

(a) A brief description of what happened, including the date of the Breach and the date of the Discovery of the Breach, if known;

(b) A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(c) Any steps the Individual should take to protect him or herself from potential harm resulting from the Breach;

(d) A brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to Individual(s), and to protect against any further Breaches; and

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

13.2 Covered Entity, in its sole discretion, may elect to provide the notification required by Section 13.1 and/or to establish the contact procedures described in Section 13.1.2.

13.3 Business Associate shall reimburse Covered Entity any and all costs incurred by Covered Entity, in complying with Subpart D of 45 C.F.R. Part 164, including but not limited to costs of notification, internet posting, or media publication, as a result of Business Associate's Breach of Unsecured Protected Health Information; Covered Entity shall not be responsible for any costs incurred by Business Associate in providing the notification required by 13.1 or in establishing the contact procedures required by Section 13.1.2.

14. DHCS REQUIREMENTS.

14.1 Business Associate and Covered Entity shall comply with the DHCS Requirements provided on **Exhibit A** and **Exhibit B** to this Business Associate Agreement with regard to DHCS PSCI and PII received from Covered Entity. To the extent that any provisions of the DHCS Requirements in Exhibit A or Exhibit B conflict with other provisions of this Business Associate Agreement, the more restrictive requirement shall apply with regard to DHCS PSCI or PII received from Covered Entity.

15. <u>INDEMNIFICATION</u>

15.1 Business Associate shall indemnify, defend, and hold harmless Covered Entity, its Special Districts, elected and appointed officers, employees, and agents from and against any and all

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

liability, including but not limited to demands, claims, actions, fees, costs, expenses (including attorney and expert witness fees), and penalties and/or fines (including regulatory penalties and/or fines), arising from or connected with Business Associate's acts and/or omissions arising from and/or relating to this Business Associate Agreement, including, but not limited to, compliance and/or enforcement actions and/or activities, whether formal or informal, by the Secretary or by the Attorney General of the State of California.

15.2 Section 15.1 is not intended by the parties to limit in any way the scope of Business Associate's obligations related to Insurance and/or Indemnification in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

16. OBLIGATIONS OF COVERED ENTITY

16.1 Covered Entity shall notify Business Associate of any current or future restrictions or limitations on the Use or Disclosure of Protected Health Information that would affect Business Associate's performance of the Services, and Business Associate shall thereafter restrict or limit its own Uses and Disclosures accordingly.

16.2 Covered Entity shall not request Business Associate to Use or Disclose Protected Health Information in any manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 or the California Confidentiality Laws if done by Covered Entity, except to the extent that Business Associate may Use or Disclose Protected Health Information as provided in Sections 2.3, 2.5, and 2.6.

17. TERM

17.1 Unless sooner terminated as set forth in Section 18, the term of this Business Associate Agreement shall be the same as the term of the applicable underlying Agreement, Contract, Participation Agreement, Master Agreement, Work Order, Purchase Order, or other service arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate. Such term shall apply to all such agreements entered into from time to time between the parties for the purpose of providing Services pursuant to the JPA.

17.2 Notwithstanding Section 17.1, Business Associate's obligations under Sections 11, 15, and 19 shall survive the termination or expiration of this Business Associate Agreement.

18. TERMINATION FOR CAUSE

18.1 In addition to and notwithstanding the termination provisions set forth in the applicable underlying Agreement, Contract, Participation Agreement, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, if either party determines that the other party has violated a material term of this Business Associate Agreement, and the breaching party has not cured the breach or ended the violation within the time specified by the non- breaching party, which shall be reasonable given the nature of the breach and/or violation, the non-breaching party may terminate this Business Associate Agreement.

18.2 In addition to and notwithstanding the termination provisions set forth in the applicable underlying Agreement, Contract, Participation Agreement, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

Contractor's status as a Business Associate, if either party determines that the other party has violated a material term of this Business Associate Agreement, and cure is not feasible, the non-breaching party may terminate this Business Associate Agreement immediately.

19. DISPOSITION OF PROTECTED HEALTH INFORMATION UPON TERMINATION OR EXPIRATION

19.1 Except as provided in Section 19.3, upon termination for any reason or expiration of this Business Associate Agreement, Business Associate shall return or, if agreed to by Covered entity, shall destroy as provided for in Section 19.2, all Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that Business Associate, including any Subcontractor, still maintains in any form. Business Associate shall retain no copies of the Protected Health Information.

19.2 Destruction for purposes of Section 19.2 and Section 6.6 shall mean that media on which the Protected Health Information is stored or recorded has been destroyed and/or electronic media have been cleared, purged, or destroyed in accordance with the use of a technology or methodology specified by the Secretary in guidance for rendering Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals.

19.3 Notwithstanding Section 19.1, in the event that return or destruction of Protected Health Information is not feasible or Business Associate determines that any such Protected Health Information is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities, Business Associate may retain that Protected Health Information for which destruction or return is infeasible or that Protected Health Information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities and shall return or destroy all other Protected Health Information.

19.3.1 Business Associate shall extend the protections of this Business Associate Agreement to such Protected Health Information, including continuing to use appropriate safeguards and continuing to comply with Subpart C of 45 C.F.R Part 164 with respect to Electronic Protected Health Information, to prevent the Use or Disclosure of such information other than as provided for in Sections 2.5 and 2.6 for so long as such Protected Health Information is retained, and Business Associate shall not Use or Disclose such Protected Health Information other than for the purposes for which such Protected Health Information was retained.

19.3.2 Business Associate shall return or, if agreed to by Covered entity, destroy the Protected Health Information retained by Business Associate when it is no longer needed by Business Associate for Business Associate's proper management and administration or to carry out its legal responsibilities.

19.4 Business Associate shall ensure that all Protected Health Information created, maintained, or received by Subcontractors is returned or, if agreed to by Covered entity, destroyed as provided for in Section 19.2.

20. AUDIT, INSPECTION, AND EXAMINATION

20.1 Covered Entity reserves the right to conduct a reasonable inspection of the facilities, systems, information systems, books, records, agreements, and policies and procedures relating to the Use or Disclosure of Protected Health Information for the purpose determining whether

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

Business Associate is in compliance with the terms of this Business Associate Agreement and any non-compliance may be a basis for termination of this Business Associate Agreement and the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, as provided for in section 18.

20.2 Covered Entity and Business Associate shall mutually agree in advance upon the scope, timing, and location of any such inspection.

20.3 At Business Associate's request, and to the extent permitted by law, Covered Entity shall execute a nondisclosure agreement, upon terms and conditions mutually agreed to by the parties.

20.4 That Covered Entity inspects, fails to inspect, or has the right to inspect as provided for in Section 20.1 does not relieve Business Associate of its responsibility to comply with this Business Associate Agreement and/or the HIPAA Rules or impose on Covered Entity any responsibility for Business Associate's compliance with any applicable HIPAA Rules.

20.5 Covered Entity's failure to detect, its detection but failure to notify Business Associate, or its detection but failure to require remediation by Business Associate of an unsatisfactory practice by Business Associate, shall not constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under this Business Associate Agreement or the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

20.6 Section 20.1 is not intended by the parties to limit in any way the scope of Business Associate's obligations related to Inspection and/or Audit and/or similar review in the applicable underlying Agreement, Contract, Participation Agreement, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

21. MISCELLANEOUS PROVISIONS

21.1 Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with the terms and conditions of this Business Associate Agreement will be adequate or satisfactory to meet the business needs or legal obligations of Business Associate.

21.2 Federal and State Requirements. The Parties agree that the provisions under HIPAA Rules and the California Confidentiality Laws that are required by law to be incorporated into this Business Associate Agreement are hereby incorporated into this Agreement.

21.3 No Third-Party Beneficiaries. Nothing in this Business Associate Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

21.4 Construction. In the event that a provision of this Business Associate Agreement is contrary to a provision of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, the provision of this Business Associate Agreement shall control. Otherwise, this Business Associate Agreement shall be construed under, and in

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

accordance with, the terms of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

21.5 Regulatory References. A reference in this Business Associate Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

21.6 Interpretation. Any ambiguity in this Business Associate Agreement shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA Rules and the California Confidentiality Laws.

21.7 Amendment. The parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the HIPAA Rules and any other privacy laws governing Protected Health Information, including the California Confidentiality Laws.

This Business Associates Agreement applies to all Participation Agreements between the County and CalMHSA.

AUTHORIZED SIGNORS:

HUMBOLDT COUNTY

Signed: Botzler-Rodgers, Emi Digitally signed by Botzler-Rodgers, Emi Date: 2022.11.16 13:50:04 -08'00' Name (Printed): Emi Botzler-Rodgers

Title: Behavioral Health Director Date: _____

Address: 720 Wood Street, Eureka, CA 95501

Phone: 707 268-2998 Email: ebotzler-rodgers@co.humboldt.ca.us

Signed: _____ Name (Printed): _____

Title: _____ Date: _____

CONTRACTOR: CALIFORNIA MENTAL HEALTH SERVICES AUTHORITY (CalMHSA)

Signed: DocuSigned by: Amie Miller 82E9EFBAB7CC446... Name (Printed): Amie Miller, Psy.D., MFT

Title: Executive Director Date: 11/20/2022

Address: 1610 Arden Way, Suite 175, Sacramento, CA 95815 Phone: (279) 234-0700

Email: amie.miller@calmhsa.org

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

Exhibit A
DHCS Information Confidentiality And Security Requirements

1. **Definitions**. For purposes of this Exhibit, the following definitions shall apply:

    a. **Public Information**: Information that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws.

    b. **Confidential Information**: Information that is exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws.

    c. **Sensitive Information**: Information that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive Information may be either Public Information or Confidential Information. It is information that requires a higher-than-normal assurance of accuracy and completeness. Thus, the key factor for Sensitive Information is that of integrity. Typically, Sensitive Information includes records of agency financial transactions and regulatory actions.

    d. **Personal Information**: Information that identifies or describes an individual, including, but not limited to, their name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It is DHCS' policy to consider all information about individuals private unless such information is determined to be a public record. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request. Personal Information includes the following:

        Notice-triggering Personal Information: Specific items of personal information (name plus Social Security number, driver license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person. For purposes of this provision, identity shall include, but not be limited to name, identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph. See Civil Code sections 1798.29 and 1798.82.

2. **Nondisclosure**. Business Associate and its employees, agents, or subcontractors shall protect from unauthorized disclosure any PSCI.

3. Business Associate and its employees, agents, or subcontractors shall not use any PSCI for any purpose other than carrying out the Business Associate 's obligations under the JPA Agreement.

4. Business Associate and its employees, agents, or subcontractors shall promptly transmit to Covered Entity's Chief Privacy Officer all requests for disclosure of any PSCI not emanating from the person who is the subject of PSCI.

5. Business Associate shall not disclose, except as otherwise specifically permitted by JPA Agreement or authorized by the person who is the subject of PSCI, any PSCI to anyone other than DHCS or Covered Entity without prior written authorization from the Covered Entity Chief Privacy Officer, except if disclosure is required by State or Federal law.

6. Business Associate shall observe the following requirements:

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

a. **Safeguards**. Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PSCI, including electronic PSCI that it creates, receives, maintains, uses, or transmits on behalf of Covered Entity. Business Associate shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of Business Associate's operations and the nature and scope of its activities, Including at a minimum the following safeguards:

i. Personnel Controls

1. ***Employee Training***. All workforce members who assist in the performance of functions or activities on behalf of Covered Entity, or access or disclose Covered Entity PSCI, must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.

2. ***Employee Discipline***. Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

3. ***Confidentiality Statement***. All persons that will be working with DHCS PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DHCS PHI or Pl. The statement must be renewed annually. Business Associate shall retain each person's written confidentiality statement for Covered Entity or DHCS inspection for a period of six (6) years following contract termination.

4. ***Background Check***. Before a member of the workforce may access DHCS PHI or PI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. Business Associate shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

ii. Technical Security Controls

1. ***Workstation/Laptop encryption***. All workstations and laptops that process and/or store DHCS PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DHCS Information Security Office.

2. ***Server Security***. Servers containing unencrypted DHCS PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

3. ***Minimum Necessary***. Only the minimum necessary amount of DHCS PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

4. ***Removable media devices***. All electronic files that contain DHCS PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

5. ***Antivirus software***. All workstations, laptops and other systems that process and/or store DHCS PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

6. ***Patch Management***. All workstations, laptops and other systems that process and/or store DHCS PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.

7. ***User IDs and Password Controls***. All users must be issued a unique user name for accessing DHCS PHI or Pl. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

    - Upper case letters (A-Z)
    - Lower case letters (a-z)
    - Arabic numerals (0-9)
    - Non-alphanumeric characters (punctuation symbols)

8. ***Data Destruction***. When no longer needed, all DHCS PHI or PI must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI or PI cannot be retrieved.

9. ***System Timeout***. The system providing access to DHCS PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

10. ***Warning Banners***. All systems providing access to DHCS PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

11. ***System Logging***. The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DHCS PHI or PI, or which alters DHCS PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If DHCS PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

12. **Access Controls**. The system providing access to DHCS PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

13. ***Transmission encryption***. All data transmissions of DHCS PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.

14. ***Intrusion Detection***. All systems involved in accessing, holding, transporting, and protecting DHCS PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

iii. Audit Controls

1. ***System Security Review***. All systems processing and/or storing DHCS PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

2. ***Log Reviews***. All systems processing and/or storing DHCS PHI or PI must have a routine procedure in place to review system logs for unauthorized access.

3. ***Change Control***. All systems processing and/or storing DHCS PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

iv. Business Continuity I Disaster Recovery Controls

1. ***Emergency Mode Operation Plan***. Business Associate must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DHCS PHI or PI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

2. ***Data Backup Plan***. Business Associate must have established documented procedures to backup DHCS PHI to maintain retrievable exact copies of DHCS PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DHCS PHI or PI should it be lost. At a minimum, the

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

schedule must be a weekly full backup and monthly offsite storage of DHCS data.

v. Paper Document Controls

1. ***Supervision of Data***. DHCS PSI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DHCS PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

2. ***Escorting Visitors***. Visitors to areas where DHCS PHI or PI is contained shall be escorted and DHCS PHI or PI shall be kept out of sight while visitors are in the area.

3. ***Confidential Destruction***. DHCS PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

4. ***Removal of Data***. DHCS PHI or PI must not be removed from the premises of the Business Associate except with express written permission of DHCS.

5. ***Faxing***. Faxes containing DHCS PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

6. ***Mailing***. Mailings of DHCS PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of DHCS PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of DHCS to use another method is obtained.

b. ***Security Officer***. Business Associate shall, to the extent it has not already done so, designate a Security Officer to oversee its data security program who will be responsible for carrying out its privacy and security programs and for communicating on security matters with Covered Entity and DHCS.

Discovery and Notification of Breach. Notice to Covered Entity:

i. To notify Covered Entity and DHCS **immediately** upon the discovery of a suspected security incident that involves data provided to Covered Entity by DHCS from the Social Security Administration. This notification will be by **telephone call plus email or fax** upon the discovery of the breach. (2) To notify Covered Entity **within 24 hours by email or fax** of the discovery of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of the JPA and this Exhibit, or potential loss of confidential data affecting the JPA. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

breach) who is an employee, officer or other agent of Business Associate.

ii. Notice shall be provided to the Covered Entity Chief Privacy Officer, the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves data provided to Covered Entity by DHCS from the Social Security Administration, notice shall be provided by calling the DHCS EITS Service Desk. Notice shall be made using the "DHCS Privacy Incident Report" form, including all information known at the time. The Business Associate shall use the most current version of this form, which is posted on the DHCS Privacy Office website (Data Privacy (ca.gov), then select "Privacy Incident Reporting Form" in the table entitled "Resources" near the middle of the page) or use this link: Privacy Incident Report (ca.gov)

c. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI, Business Associate shall take:

i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment and

ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

d. ***Investigation of Breach***. Business Associate shall immediately investigate such security incident, breach, or unauthorized use or disclosure of PSCI. If the initial report did not include all of the requested information marked with an asterisk, then within seventy-two (72) hours of the discovery, Business Associate shall submit an updated "DHCS Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Covered Entity Chief Privacy Officer, the DHCS Privacy Officer, and the DHCS Information Security Officer:

e. ***Written Report***. Business Associate shall provide a written report of the investigation to the Covered Entity Chief Privacy Officer, the DHCS Privacy Officer, and the DHCS Information Security Officer, if all of the required information was not included in the DHCS Privacy Incident Report, within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.

f. ***Notification of Individuals***. Business Associate shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The Covered Entity Chief Privacy Officer, the DHCS Privacy Officer, and the DHCS Information Security Officer shall approve the time, manner and content of any such notifications.

7. **Effect on lower tier transactions**. The terms of this Exhibit shall apply to all contracts, subcontracts, and subawards, regardless of whether they are for the acquisition of services, goods, or commodities. Business Associate shall incorporate the contents of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.

8. **Contact Information**. To direct communications to the above referenced Covered Entity or DHCS staff, Business Associate shall initiate contact as indicated herein. Covered Entity reserves the right to make changes to the contact information below by giving written notice to Business Associate. Said changes

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

shall not require an amendment to this Exhibit or the JPA Agreement to which it is incorporated.

Covered Entity Chief Privacy Officer	**DHCS Privacy Officer**	**DHCS Information Security Officer**
See Section 5.2.2 of this Business Associate Agreement for Covered Entity contact information.	Privacy Officer c/o Office of Legal Services Department of Health Care Services P.O. Box 997413, MS 0011 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95889-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Help Desk (916) 440-7000 or (800) 579-0874

9. **Audits and Inspections**. From time to time, DHCS may inspect the facilities, systems, books and records of the Business Associate to monitor compliance with the safeguards required in the Information Confidentiality and Security Requirements (ICSR) exhibit. Business Associate shall promptly remedy any violation of any provision of this ICSR exhibit. The fact that DHCS inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this ICSR exhibit.

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

Exhibit B

Privacy and Information Security Provisions

This Exhibit B is intended to protect the privacy and security of specified DHCS information that Business Associate may access, receive, or transmit under the JPA Agreement. The DHCS information covered under this Exhibit B consists of: (1) PHI and (2) PI. PI may include data provided to DHCS by the Social Security Administration.

Exhibit B consists of the following parts:

1. Exhibit B-1 provides for the privacy and security of PI under Civil Code Section 1798.3(a) and 1798.29.

2. Exhibit B-2, Miscellaneous Provisions, sets forth additional terms and conditions that extend to the provisions of Exhibit B in its entirety.

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

Exhibit B-1
Privacy and Security of Personal Information and
Personally Identifiable Information Not Subject to HIPAA

1. Recitals.

a. In addition to the Privacy and Security Rules under HIPAA, DHCS is subject to various other legal and contractual requirements with respect to the personal information (as defined in section 2 below) and personally identifiable information (as defined in section 2 below) it maintains. These include:

i. The California Information Practices Act of 1977 (California Civil Code §§1798 et seq.),

ii. Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2.

b. The purpose of this Exhibit B-1 is to set forth Business Associate's privacy and security obligations with respect to PI and PII that Business Associate may create, receive, maintain, use, or disclose for or on behalf of Covered Entity pursuant to the JPA Agreement. Specifically, this Exhibit applies to PI and PII which is not PHI as defined by HIPAA and therefore is not addressed in this Business Associate Agreement; however, to the extent that data is both PHI or ePHI and PII, both the Business Associate Agreement and this Exhibit B-1 shall apply.

c. The terms used in this Exhibit B-1, but not otherwise defined, shall have the same meanings as those terms have in the above referenced statute and agreement. Any reference to statutory, regulatory, or contractual language shall be to such language as in effect or as amended.

2. Definitions. The following definitions apply to such terms used in this Exhibit B-1. Abbreviated and capitalized terms used in this Exhibit but not defined below shall have the meaning ascribed to them under this Business Associate Agreement.

a. "Breach" shall have the meaning given to such term under the CMPPA (as defined below in Section 2(c)). It shall include a "PII loss" as that term is defined in the CMPPA.

b. "Breach of the security of the system" shall have the meaning given to such term under the California Information Practices Act, Civil Code section 1798.29(f).

c. "CMPPA Agreement" means the Computer Matching and Privacy Protection Act ("CMPPA") Agreement between the Social Security Administration and the California Health and Human Services Agency ("CHHS").

d. "DHCS PI" shall mean Personal Information, as defined below, accessed in a database maintained by the DHCS, received by Business Associate from Covered Entity or acquired or created by Business Associate in connection with performing the functions, activities and services specified in the JPA Agreement on behalf of the Covered Entity.

e. "Notice-triggering Personal Information" shall mean the personal information identified in Civil Code section 1798.29 whose unauthorized access may trigger notification requirements under Civil Code section 1798.29. For purposes of this provision, identity shall include, but not be limited to, name, address, email address, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, a photograph or a biometric identifier. Notice-triggering Personal Information includes PI in electronic, paper or any other medium.

f. "Personally Identifiable Information" ("PII") shall have the meaning given to such term in the

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

CMPPA.

g. "Personal Information" ("PI") shall have the meaning given to such term in California Civil Code Section 1798.3(a).

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

i. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PI, or confidential data utilized in complying with the JPA Agreement; or interference with system operations in an information system that processes, maintains or stores PI.

3. Terms of Agreement

a. Permitted Uses and Disclosures of DHCS PI and PII by Business Associate

Except as otherwise indicated in this Exhibit B-1, Business Associate may use or disclose DHCS PI only to perform functions, activities or services for or on behalf of the DHCS pursuant to the terms of the JPA Agreement provided that such use or disclosure would not violate the California Information Practices Act ("CIPA") if done by the DHCS.

b. Responsibilities of Business Associate

Business Associate agrees:

i. **Nondisclosure**. Not to use or disclose DHCS PI or PII other than as permitted or required by the JPA Agreement or as required by applicable state and federal law.

ii. **Safeguards**. To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of DHCS PI and PII, to protect against anticipated threats or hazards to the security or integrity of DHCS PI and PII, and to prevent use or disclosure of DHCS PI or PII other than as provided for by the JPA Agreement. Business Associate shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Business Associate's operations and the nature and scope of its activities, which incorporate the requirements of section (c), Security, below. Business Associate will provide Covered Entity or DHCS with its current policies upon request.

c. **Security**. Business Associate shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or Pl. These steps shall include, at a minimum:

i. Complying with all of the data system security precautions listed in Attachment A, Business

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

Associate Data Security Requirements;

ii. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

iii. If the data obtained by Business Associate from DHCS through Covered Entity includes PII, Contractor shall also comply with the substantive privacy and security requirements in the CMPPA Agreement. Business Associate also agrees to ensure that any agents, including a subcontractor to whom it provides DHCS PII, agree to the same requirements for privacy and security safeguards for confidential data that apply to Business Associate with respect to such information.

d. **Mitigation of Harmful Effects**. To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of DHCS PI or PII by Business Associate or its subcontractors in violation of this Exhibit B-1.

e. **Business Associate's Agents and Subcontractors**. To impose the same restrictions and conditions set forth in this Exhibit B-1 on any subcontractors or other agents with whom Business Associate subcontracts any activities under the JPA Agreement that involve the disclosure of DHCS PI or PII to the subcontractor.

f. **Availability of Information to Covered Entity and DHCS**. To make DHCS PI and PII available to Covered Entity or DHCS for purposes of oversight, inspection, amendment, and response to requests for records, injunctions, judgments, and orders for production of DHCS PI and PII. If Business Associate receives DHCS PII, upon request by Covered Entity or DHCS, Business Associate shall provide Covered Entity or DHCS, as applicable, with a list of all employees, contractors and agents who have access to DHCS PII, including employees, contractors and agents of its subcontractors and agents.

g. **Cooperation with Covered Entity and DHCS**. With respect to DHCS PI, to cooperate with and assist the Covered Entity or DHCS, as applicable, to the extent necessary to ensure DHCS's compliance with the applicable terms of the CIPA including, but not limited to, accounting of disclosures of DHCS PI, correction of errors in DHCS PI, production of DHCS PI, disclosure of a security breach involving DHCS PI and notice of such breach to the affected individual(s).

h. **Confidentiality of Alcohol and Drug Abuse Patient Records**. Business Associate agrees to comply with all confidentiality requirements set forth in Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2. Business Associate is aware that criminal penalties may be imposed for a violation of these confidentiality requirements.

i. **Breaches and Security Incidents**. During the term of this Agreement, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

i. Initial Notice to Covered Entity. (1) To notify Covered Entity and DHCS immediately by telephone call or email or fax upon the discovery of a breach of unsecured DHCS PI or PII in electronic media or in any other media if the PI or PII was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon discovery of a suspected security incident involving DHCS PII. (2) To notify Covered Entity and DHCS within 24 hours by email or fax of the discovery of any suspected security incident, intrusion or unauthorized

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

access, use or disclosure of DHCS PI or PII in violation of the JPA Agreement or this Exhibit B-1 or potential loss of confidential data affecting the JPA Agreement. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.

ii. Notice shall be provided to the Covered Entity Chief Privacy Officer and DHCS Information Protection Unit, Office of HIPAA Compliance. If the incident occurs after business hours or on a weekend or holiday and involves electronic DHCS PI or PII, notice shall be provided to DHCS by calling the DHCS Information Security Officer. Notice to DHCS shall be made using the DHCS "Privacy Incident Report" form, including all information known at the time. Business Associate shall use the most current version of this form, which is posted on the DHCS Information Security Officer website (Data Privacy (ca.gov), then select the "Privacy Incident Reporting Form" in the table entitled "Resources" or use this link: Privacy Incident Report (ca.gov).

iii. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of DHCS PI or PII, Business Associate shall take:

1. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

2. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

iv. **Investigation and Investigation Report**. To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI. Within 72 hours of the discovery, Business Associate shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the DHCS Information Security Officer.

v. **Complete Report**. To provide a complete report of the investigation to Covered Entity and the DHCS Information Protection Unit within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report to DHCS shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If DHCS requests information in addition to that listed on the "Privacy Incident Report" form, Business Associate shall make reasonable efforts to provide Covered Entity or DHCS, as applicable, with such information. If, because of the circumstances of the incident, Business Associate needs more than ten (10) working days from the discovery to submit a complete report, the DHCS may grant a reasonable extension of time, in which case Business Associate shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. DHCS will review and approve the determination of whether a breach occurred and whether individual notifications and a corrective action plan are required.

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

vi. **Responsibility for Reporting of Breaches**. If the cause of a breach of DHCS PI or PII is attributable to Business Associate or its agents, subcontractors or vendors, Business Associate is responsible for all required reporting of the breach as specified in CIPA, section 1798.29. Business Associate shall bear all costs of required notifications to individuals as well as any costs associated with the breach. The Privacy Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made. Covered Entity or DHCS, as applicable, will provide its review and approval expeditiously and without unreasonable delay.

vii. If Business Associate has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors or Covered Entity may report the breach or incident to DHCS in addition to Business Associate , Business Associate shall notify DHCS, and DHCS, Covered Entity, and Business Associate may take appropriate action to prevent duplicate reporting.

viii. **DHCS and Covered Entity Contact Information**. To direct communications to the above referenced Covered Entity and DHCS staff, Business Associate shall initiate contact as indicated herein. Covered Entity reserves the right to make changes to the contact information below by giving written notice to the Business Associate . Said changes shall not require an amendment to this Exhibit or the JPA Agreement to which it is incorporated.

Covered Entity Chief Privacy Officer	**DHCS Privacy Officer**	**DHCS Information Security Officer**
See Section 5.2.2 of this Business Associate Agreement for Covered Entity contact information.	Privacy Officer c/o Office of Legal Services Department of Health Care Services P.O. Box 997413, MS 0011 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95889-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Help Desk (916) 440-7000 or (800) 579-0874

j. Designation of Individual Responsible for Security

Business Associate shall designate an individual, (e.g., Security Officer), to oversee its data security program who shall be responsible for carrying out the requirements of this Exhibit B-1 and for communicating on security matters with Covered Entity and DHCS.

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

Exhibit B-2
Miscellaneous Terms and Conditions
Applicable to Exhibit B

1. **Disclaimer.** Covered Entity makes no warranty or representation that compliance by Business Associate with this Exhibit B, HIPAA or the HIPAA regulations will be adequately or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of the DHCS PHI, PI and PII.

2. **Amendment.** The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Exhibit B may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations, and other applicable state and federal laws. Upon either party's request, the other party agrees to promptly enter into negotiations concerning an amendment to this Exhibit B embodying written assurances consistent with requirements of HIPAA, the HITECH Act, and the HIPAA regulations, and other applicable state and federal laws. Covered Entity may terminate the JPA Agreement upon thirty (30) days written notice in the event:

    a. Business Associate does not promptly enter into this Exhibit B when requested by Covered Entity; or

    b. Business Associate does not enter into an amendment providing assurances regarding the safeguarding of DHCS PHI that the DHCS deems is necessary to satisfy the standards and requirements of HIPAA and the HIPAA regulations

3. **Judicial or Administrative Proceedings**. Business Associate will notify Covered Entity and DHCS if it is named as a defendant in a criminal proceeding for a violation of HIPAA or other security or privacy law. Covered Entity may at the request of DHCS terminate the JPA Agreement if Business Associate is found guilty of a criminal violation of HIPAA. Covered Entity may at the request of DHCS terminate the JPA Agreement if a finding or stipulation that Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined. DHCS will consider the nature and seriousness of the violation in deciding whether or not to request that Covered Entity terminate the JPA Agreement.

4. **Assistance in Litigation or Administrative Proceedings**. Business Associate shall make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under the JPA Agreement, available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers or employees based upon claimed violation of HIPAA, or the HIPAA regulations, which involves inactions or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named adverse party.

5. **No Third-Party Beneficiaries**. Nothing express or implied in the terms and conditions of this Exhibit B is intended to confer, nor shall anything herein confer, upon any person other than the Covered Entity or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

6. **Interpretation**. The terms and conditions in this Exhibit B shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, and the HIPAA regulations. The parties agree

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

that any ambiguity in the terms and conditions of this Exhibit B shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations, and, if applicable, any other relevant state and federal laws.

7. **Conflict**. In case of a conflict between any applicable privacy or security rules, laws, regulations or standards the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI, PI and PII from unauthorized disclosure. Further, Business Associate must comply within a reasonable period of time with changes to these standards that occur after the effective date of the JPA Agreement.

8. **Regulatory References**. A reference in the terms and conditions of this Exhibit B to a section in the HIPAA regulations means the section as in effect or as amended.

9. **Survival**. The respective rights and obligations of Business Associate under Item 3(b) of Exhibit B-1, Responsibilities of Business Associate, shall survive the termination or expiration of this Agreement.

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

11. **Audits, Inspection and Enforcement**. From time to time, and subject to all applicable federal and state privacy and security laws and regulations, Covered Entity or DHCS may conduct a reasonable inspection of the facilities, systems, books and records of to monitor compliance with this Exhibit B. Business Associate shall promptly remedy any violation of any provision of this Exhibit B. The fact that Covered Entity or DHCS inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Exhibit B. Covered Entity's or DHCS's failure to detect a non-compliant practice, or a failure to report a detected noncompliant practice to Business Associate does not constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under the JPA Agreement or related documents, including this Exhibit B.

12. **Due Diligence**. Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Exhibit B and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and other applicable state and federal law, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Exhibit B.

13. **Term**. The Term of this Exhibit B shall extend beyond the termination of the Agreement and shall terminate when all DHCS PHI is destroyed or returned to Covered Entity, in accordance with 45 CFR Section 1 64.504(e)(2)(ii)(1), and when all DHCS PI and PII is destroyed in accordance with Attachment A.

14. **Effect of Termination**. Upon termination or expiration of this Agreement for any reason, Business Associate shall return or destroy all DHCS PHI, PI and PII that Business Associate still maintains in any form, and shall retain no copies of such PHI, PI or PII. If return or destruction is not feasible, Business Associate shall notify Covered Entity an DHCS of the conditions that make the return or destruction infeasible, and Covered Entity, DHCS, and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI, PI or PII. Business Associate shall continue to extend the protections of this Exhibit B to such DHCS PHI, PI and PII, and shall limit further use of such data to those purposes that make the return or destruction of such data infeasible. This provision shall apply to DHCS PHI, PI and PII that is in the possession of subcontractors or agents of Business Associate.

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

Attachment A
Data Security Requirements

1. Personnel Controls

a. **Employee Training**. All workforce members who assist in the performance of functions or activities on behalf of the Covered Entity with respect to DHCS-provided information, or access or disclose DHCS PHI or PI must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following termination of this Agreement.

b. **Employee Discipline**. Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

c. **Confidentiality Statement**. All persons that will be working with DHCS PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DHCS PHI or Pl. The statement must be renewed annually. Business Associate shall retain each person's written confidentiality statement for Covered Entity or DHCS inspection for a period of six (6) years following termination of this Agreement.

d. **Background Check**. Before a member of the workforce may access DHCS PHI or PI, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. Business Associate shall retain each workforce member's background check documentation for a period of three (3) years.

2. Technical Security Controls

a. **Workstation/Laptop encryption**. All workstations and laptops that store DHCS PHI or PI either directly or temporarily must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DHCS Information Security Office.

b. **Server Security**. Servers containing unencrypted DHCS PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

c. **Minimum Necessary**. Only the minimum necessary amount of DHCS PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

d. **Removable media devices**. All electronic files that contain DHCS PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

e. **Antivirus software**. All workstations, laptops and other systems that process and/or store DHCS PHI or PI must install and actively use comprehensive anti-virus software solution with

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

automatic updates scheduled at least daily.

f. **Patch Management**. All workstations, laptops and other systems that process and/or store DHCS PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release. Applications and systems that cannot be patched within this time frame due to significant operational reasons must have compensatory controls implemented to minimize risk until the patches can be installed. Applications and systems that cannot be patched must have compensatory controls implemented to minimize risk, where possible.

g. **User IDs and Password Controls**. All users must be issued a unique user name for accessing DHCS PHI or Pl. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed at least every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

h. Upper case letters (A-Z)

i. Lower case letters (a-z)

j. Arabic numerals (0-9)

k. Non-alphanumeric characters (punctuation symbols)

l. **Data Destruction**. When no longer needed, all DHCS PHI or PI must be wiped using the Gutmann or US DHCS of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the DHCS Information Security Office.

m. **System Timeout**. The system providing access to DHCS PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

n. **Warning Banners**. All systems providing access to DHCS PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

o. **System Logging**. The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DHCS PHI or PI, or which alters DHCS PHI or Pl. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If DHCS PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

p. **Access Controls**. The system providing access to DHCS PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

q. **Transmission encryption**. All data transmissions of DHCS PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing DHCS PHI can be encrypted. This requirement pertains to any type of DHCS PHI or PI in motion such as website access, file transfer, and E-Mail.

r. **Intrusion Detection**. All systems involved in accessing, holding, transporting, and protecting DHCS PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. Audit Controls

a. **System Security Review**. Business Associate must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing DHCS PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

b. **Log Reviews**. All systems processing and/or storing DHCS PHI or PI must have a routine procedure in place to review system logs for unauthorized access.

c. **Change Control**. All systems processing and/or storing DHCS PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4. Business Continuity / Disaster Recovery Controls

a. **Emergency Mode Operation Plan**. Business Associate must establish a documented plan to enable continuation of critical business processes and protection of the security of DHCS PHI or PI held in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

b. **Data Backup Plan**. Business Associate must have established documented procedures to backup DHCS PHI to maintain retrievable exact copies of DHCS PHI or Pl. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DHCS PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

5. Paper Document Controls

a. **Supervision of Data**. DHCS PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DHCS PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

b. **Escorting Visitors**. Visitors to areas where DHCS PHI or PI is contained shall be escorted and DHCS PHI or PI shall be kept out of sight while visitors are in the area.

c. **Confidential Destruction**. DHCS PHI or PI must be disposed of through confidential means, such as crosscut shredding and pulverizing.

DocuSign Envelope ID: CE4E0ACD-5E85-4C1A-86F9-2B1316D82813

d. **Removal of Data**. Only the minimum necessary DHCS PHI or PI may be removed from the premises of Business Associate except with express written permission of DHCS. DHCS PHI or PI shall not be considered "removed from the premises" if it is only being transported from one of Business Associate's locations to another of Business Associates locations.

e. **Faxing**. Faxes containing DHCS PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

f. **Mailing**. Mailings containing DHCS PHI or PI shall be sealed and secured from damage or inappropriate viewing of such PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of DHCS PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of DHCS to use another method is obtained.