

CALIFORNIA MENTAL HEALTH SERVICES AUTHORITY
PARTICIPATION AGREEMENT
DATA ARCHIVE SOLUTION PROGRAM
COVER SHEET

This Participation Agreement No. 5127-ARCHIVE-2023-SB ("Agreement") is entered into between the California Mental Health Services Authority ("CalMHSA"), a Joint Powers Authority, and County of Santa Barbara, a political subdivision of the State of California, on behalf of its Department of Behavioral Wellness ("Participant"), each at times individually referred to as "Party" or collectively as "Parties", wherein CalMHSA agrees to provide, and Participant agrees to accept, the services specified herein.

WHEREAS, CalMHSA represents that it is specially trained, skilled, experienced, and competent to perform the special services required by Participant, and Participant desires to retain the services of CalMHSA pursuant to the terms, covenants, and conditions herein set forth.

NOW, THEREFORE, in consideration of the mutual covenants, terms, and conditions contained herein, the Parties agree as follows:

1. Participant desires to participate in the Program identified below.

Name of Program: Data Archive Solution

Summary of Program: CalMHSA will provide Participant with a Microsoft Azure Cloud database solution and professional implementation and support services to assist with archiving legacy application electronic health record ("EHR") databases to a secure Cloud environment. Through this Program, CalMHSA strives to help Participant retain copies of and access to legacy EHR data, while also assisting Participant in taking steps toward meeting future interoperability requirements.

2. CalMHSA and Participant acknowledge that the Program will be governed by CalMHSA's Joint Powers Agreement and its Bylaws, and by this Agreement. The following exhibits, all of which are attached hereto and incorporated herein by reference, are intended to clarify how the provisions of those documents will be applied to this Program.

<input checked="" type="checkbox"/>	Exhibit A	Program Description and Funding
<input checked="" type="checkbox"/>	Exhibit B	General Terms and Conditions
<input checked="" type="checkbox"/>	Exhibit C	Data Sharing Agreement
<input checked="" type="checkbox"/>	Exhibit BAA	Business Associate Agreement

3. In full consideration for CalMHSA's services, CalMHSA will be paid a total maximum contract amount not to exceed \$79,704 in accordance with the terms of Exhibit A.
4. **Term.** The term of the Program is January 1, 2024, through December 31, 2026.
5. **Precedence.** In the event of conflict between the provisions contained in the numbered sections of this Agreement and the provisions contained in the Exhibits, the provisions of the Exhibits shall prevail over those in the numbered sections.

Agreement No. 5127-ARCHIVE-2023-SB

Data Archive Solution

August 6, 2025

6. **Execution of Counterparts.** This Agreement may be executed in any number of counterparts and each of such counterparts shall for all purposes be deemed to be an original; and all such counterparts, or as many of them as the Parties shall preserve undestroyed, shall together constitute one and the same instrument.

7. **Authority.** All signatories and parties to this Agreement warrant and represent that they have the power and authority to enter into this Agreement in the names, titles and capacities herein stated and on behalf of any entities, persons, or firms represented or purported to be represented by such entity(ies), person(s), or firm(s) and that all formal requirements necessary or required by any state and/or federal law in order to enter into this Agreement have been fully complied with. Furthermore, by entering into this Agreement, Contractor hereby warrants that it shall not have breached the terms or conditions of any other contract or agreement to which Contractor is obligated, which breach would have a material effect hereon.

THIS SECTION LEFT BLANK INTENTIONALLY

SIGNATURE PAGE FOLLOWS


Agreement No. 5127-ARCHIVE-2023-SB

Data Archive Solution

August 6, 2025

Authorized Signatures:

CalMHSA:

Signed:  DocuSigned by: _____ Name (Printed): Dr. Amie Miller, Psy.D., MFT
82E9EFB87CC446...

Participant (County of Santa Barbara):

COUNTY OF SANTA BARBARA:

By: _____
LAURA CAPPS, CHAIR
BOARD OF SUPERVISORS

Date: _____

ATTEST:


MONA MIYASATO
COUNTY EXECUTIVE OFFICER
CLERK OF THE BOARD

By: _____
Deputy Clerk

Date: _____

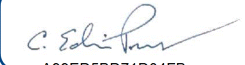
APPROVED AS TO FORM:

RACHEL VAN MULLEM
COUNTY COUNSEL

By:  Signed by: _____
48A252DEFFD3400...
Deputy County Counsel

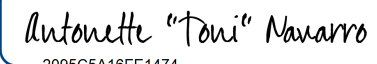
APPROVED AS TO ACCOUNTING FORM:

BETSY M. SCHAFER, CPA
AUDITOR-CONTROLLER

By:  Signed by: _____
A09ED6BD74D04FB...
Deputy

RECOMMENDED FOR APPROVAL:

ANTONETTE NAVARRO, LMFT, DIRECTOR
DEPARTMENT OF BEHAVIORAL WELLNESS

By:  DocuSigned by: _____
2095C5A16FE1474...
Director

APPROVED AS TO FORM:

GREG MILLIGAN, ARM
RISK MANAGER

By:  DocuSigned by: _____
05F565F00260466...
Risk Manager

Participation Agreement

EXHIBIT A – PROGRAM DESCRIPTION AND FUNDING

I. Name of Program: Data Archive Solution

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

III. Scope of Work:

CalMHSA will deliver to Participant a functional technical solution for archiving legacy application EHR databases utilizing a Microsoft Azure SQL Cloud database.

A. CalMHSA Responsibilities

CalMHSA will provide Participant the following professional services:

1. Planning and Coordination – In coordination with Participant, CalMHSA will create and deliver plan-based materials and any applicable documents associated with the planning and deployment of the Program within 120 calendar days of CalMHSA's receipt of archival data from Participant.
2. Project Management – In collaboration with Participant, CalMHSA Project Managers will facilitate the scope of the project and provide direction and oversight of deliverables within anticipated timelines. CalMHSA will make commercially reasonable efforts to make available the Participant's archive within thirty (30) calendar days of receipt of data. Should CalMHSA not be able to make this timeline, CalMHSA will communicate to Participant as such and provide an updated delivery timeline, subject to acknowledgment by Participant's designated project representative. Deliverables include, but are not limited to, an active cloud-hosted archive.
3. Architecture and Design - CalMHSA will architect and design the Microsoft Azure SQL Cloud environment using accepted best practices.
4. Data Migration - CalMHSA will perform all data migration activities for Participant after Participant has transferred its archive database in a structured format. CalMHSA will provide Participant with an estimated timeline for completion within thirty (30) calendar days of database restoration. Normalization is expected to take approximately six (6) to nine (9) months to complete.
5. Testing and Validation - CalMHSA representatives will connect to each data set including Sharecare and Clinician's Gateway, and confirm successful migration. If any issues are found, CalMHSA will address, resolve and re-validate.
6. Participant Database Access - CalMHSA will ensure that Participant has read only access to the Microsoft Azure SQL database. This level of access will facilitate Participant's ability to access data and allow Participant to create reports as needed.
7. Database Maintenance and Back-Up - CalMHSA will maintain the Microsoft Azure SQL Cloud environment and ensure annual back-up of database.

8. Uptime and Support

- i. CalMHSA will provide email support Monday through Friday, 8:00 a.m. to 5:00 p.m. PST. For any support questions please email: connex@calmhsa.org.
- ii. The services may occasionally become temporarily unavailable for maintenance purposes. CalMHSA will make commercially reasonable efforts to minimize any such unavailability. CalMHSA will provide Participant with five (5) business days' advance written notice of planned outages. Issues resulting in a system outage will be acknowledged and communicated within 4 hours of identification. CalMHSA will provide written root cause of analysis of outage upon Participant's request.
- iii. Uptime
 1. General Service Level Requirements – the percentage per year during which the service is available and operative for Participant use: Ninety-nine Percent (99%).
 2. Service Hours – The hours during which services are expected to be provided. The Data Archiving Solution Service Hours shall be all hours.
 3. Service Response and Resolution Times – In the event of service unavailability discovered by Participant, CalMHSA shall respond to Participant within 24 business hours of email notification of such service unavailability. CalMHSA shall resolve service unavailability by permanent fix or acceptable workaround within thirty (30) days of notice of service unavailability.

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. Report Creation – Participant is responsible for the creation of any required reports utilizing Participant's database access. CalMHSA offers additional services upon request to assist Participant in report creation.
3. Project Management and Coordination – Participant agrees to assign staff to communicate and collaborate with CalMHSA throughout the archiving project.

IV. Fees

- A. Payment for Program services shall be made upon CalMHSA's performance conforming with the scope and methodology contained in this Exhibit A as determined by Participant, in its reasonable discretion.
- B. Quarterly, CalMHSA shall submit to ap@sbcbswell.org an invoice for the service performed over the period specified. These invoices must cite the assigned agreement number. Participant shall evaluate the quality of the service performed subject to the terms of this Agreement. If

Participant, in its reasonable discretion, determines that CalMHSA's services have not conformed to the terms of this Agreement Participant shall provide CalMHSA with written notice of nonconformity and a reasonable opportunity to cure. Participant shall pay invoices for satisfactory work within 30 days of receipt of conforming and complete invoices from CalMHSA.

- C. Participant's failure to discover or object to any unsatisfactory work or billings prior to payment will not constitute a waiver of Participant's right to require CalMHSA to correct such work or billings or seek any other legal remedy.

D. Rate Table:

SERVICE TYPE	ONE-TIME FEE
Data Archiving Solution – Professional Services and Implementation <ul style="list-style-type: none"> Planning and Coordination Project Management Architecture and Design Data Migration Testing and Validation Participant Access to Azure SQL Database Database Maintenance and Backup 	\$24,900.00
LICENSE FEE	ANNUAL RATE
Data Archiving Solution – Database License Fee <ul style="list-style-type: none"> Microsoft Azure SQL Single Database License West US Region for Low Latency 4V Cores Provisioned Database Gen 5 Server Zone-Redundancy 100 Hours Compute Time Per Month RA-GRS Backup Storage Redundancy 1024GB Long Term Retention Long Term Storage with Annual Backup 	\$11,268.00 per Year
OPTIONAL ADDITIONAL SERVICES	RATE
Additional Professional Service Offering <ul style="list-style-type: none"> Report Writing 	\$225.00 per Hour
Additional Data Storage and Back-Up <ul style="list-style-type: none"> 512 GB Per Month Includes 2 Additional V Cores Per 512 GB 	\$396 per Month

Fiscal Year	APPLICABLE FISCAL PERIOD	One-Time Fee	Quarterly Rate	TOTAL AMOUNT
1	1/1/24 – 6/30/24	\$24,900	\$2,817	\$30,534
2	7/1/24 – 6/30/25		\$2,817	\$11,268
3	7/1/25 – 6/30/26		\$2,817	\$11,268
4	7/1/26 – 12/31/26		\$2,817	\$5,634
Optional Additional Services				
Report Writing; and Data Storage and Back-up				\$21,000
				\$79,704

- V. The total maximum contract amount payable for the term of this Agreement is \$79,704. Any purchase that will increase the total maximum contract amount payable under this agreement must be agreed upon in a written contract signed by the Parties.

This amount is comprised of a \$24,900 one-time fee plus an \$11,268 annual subscription fee. Participant may choose to purchase optional additional services, described in Exhibit A, Section IV.D Fees, Rate Table, Optional Additional Services. Purchase of Optional Additional Services must be in writing, and may not exceed a total amount of \$21,000.

THIS SECTION LEFT BLANK INTENTIONALLY

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. In reference to the Party to this Agreement, Participant shall mean the County of Santa Barbara.
- D. Program – The program identified in the Cover Sheet.

II. Responsibilities

- A. Responsibilities of CalMHSA:
 - 1. Manage funds received consistent with the requirements of any applicable laws, regulations, guidelines and/or contractual obligations.
 - 2. Provide regular fiscal reports to Participant and/or other public agencies with a right to such reports.
 - 3. Comply with applicable laws, regulations, guidelines, and contractual agreements and 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. Provide feedback on Program performance.
 - 4. Comply with applicable laws, regulations, guidelines, contractual agreements, JPAs, and bylaws.

III. Access and Use

Provision of Access. CalMHSA hereby grants Participant a non-exclusive, non-transferable right to access and use the Program services ("Services") during the Term, solely for use by Participant's employees who are authorized by Participant to access and use the Services under the rights granted to Participant under this Agreement ("Authorized Users") in accordance with the terms and conditions herein. Such use is limited to Participant's internal use. CalMHSA shall promptly provide to Participant the necessary passwords and network links or connections to allow Participant to access the Services.

IV. Service Levels and Support

CalMHSA shall make the Services available in accordance with the service levels set out in Exhibit A. Throughout the Term, CalMHSA shall maintain a business continuity and disaster recovery plan for the Services and implement such plan in the event of any unplanned interruption of the Services.

V. Fees and Payment

Participant shall pay CalMHSA the fees ("Fees") set forth in Exhibit A. CalMHSA shall invoice Participant for all Fees in accordance with the invoicing schedule and requirements set forth in Exhibit A. Participant shall pay all undisputed invoices within 30 days after Participant's receipt of a conforming invoice.

VI. Warranties and Warranty Disclaimer

CalMHSA warrants that during the Term of this Agreement, the Services or other items provided by CalMHSA hereunder (i) will conform in all material respects to the specifications set forth in Exhibit A during the Term of this Agreement; (ii) will be provided in compliance with all applicable laws; (iii) do not contain any virus or other malicious code; and (iv) does not infringe upon the intellectual or other proprietary rights of any third party.

EXCEPT FOR THE WARRANTIES SET FORTH IN THIS SECTION VI WARRANTIES AND WARRANTY DISCLAIMER, 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.

VII. Indemnification and Insurance**A. INDEMNIFICATION**

In lieu of and notwithstanding the pro rata risk allocation which might otherwise be imposed between the Parties pursuant to California Government Code Section 895.6, the Parties agree that all losses or liabilities incurred by a Party shall not be shared pro rata but instead all Parties agree that pursuant to California Government Code Section 895.4, each of the Parties hereto shall fully indemnify and hold each of the other Parties, their officers, board members, employees and agents, harmless from any claim, expense or cost, damage or liability imposed for injury (as defined by California Government Code Section 810.8) occurring by reason of the negligent acts or omissions or willful misconduct of the indemnifying Party, its officers, board members, employees or agents, under or in connection with or arising out of any work, authority or jurisdiction delegated to such Party under this Agreement. No Party, nor any officer, board member, employee or agent thereof shall be responsible for any damage or liability occurring by reason of the negligent acts or omissions or willful misconduct of other Parties hereto, their officers, board members, employees or agents, under or in connection with or arising out of any work, authority or jurisdiction delegated to such other Parties under this Agreement.

B. INSURANCE

Each party shall maintain its own insurance coverage, through commercial insurance, self-insurance or a combination thereof, against any claim, expense, cost, damage, or liability arising out of the performance of its responsibilities pursuant to this Agreement.

VIII. Limitation of Liability

EXCEPT AS OTHERWISE PROVIDED IN THIS AGREEMENT, 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. The exclusions and limitations in this Section VIII. Limitation of Liability do not apply to claims pursuant to Sections VII Indemnification and Insurance, X Miscellaneous I Property and Participant Information , and BAA indemnification section 15.

IX. Withdrawal, Cancellation, and Termination

- A. By Participant. Participant may, by written notice to CalMHSA, terminate this Agreement in whole or in part at any time, whether for Participant's convenience, for nonappropriation of funds, or because of the failure of CalMHSA to fulfill the obligations herein.
 - 1. For Convenience: 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.
 - 2. For Nonappropriation of Funds. The Parties acknowledge and agree that this Agreement is dependent upon the availability of County, State, and/or federal funding.
 - a. If funding to make payments in accordance with the provisions of this Agreement is not forthcoming from the County, State and/or federal governments for the Agreement, or is not allocated or allotted to County by the County, State and/or federal governments for this Agreement for periodic payment in the current or any future fiscal period, then the obligations of Participant to make payments after the effective date of such non-allocation or non-funding, as provided in the notice, will cease and terminate.
 - b. As permitted by applicable State and Federal laws regarding funding sources, if funding to make payments in accordance with the provisions of this Agreement is delayed or is reduced from the County, State, and/or federal governments for the Agreement, or is not allocated or allotted in full to County by the County, State, and/or federal governments for this Agreement for periodic payment in the current or any future fiscal period, then the obligations of Participant to make payments will be delayed or be reduced accordingly or Participant shall have the right to terminate the Agreement. If such funding is reduced, Participant in its sole discretion shall determine which aspects of the Agreement shall proceed and which Services shall be performed. In these situations, Participant will pay CalMHSA for Services and Deliverables and certain of its costs. Any obligation to pay by Participant will not extend beyond the end of Participant's then-current funding period.
 - c. CalMHSA expressly agrees that no penalty or damages shall be applied to, or shall accrue to, Participant in the event that the necessary funding to pay under the terms of this Agreement is not available, not allocated, not allotted, delayed or reduced.

3. For Cause. Should CalMHSA default in the performance of this Agreement or materially breach any of its provisions, Participant may, at Participant's sole option, terminate or suspend this Agreement in whole or in part after providing CalMHSA with written notice of said default or material breach and a 30-day opportunity to cure. If CalMHSA does not cure within the prescribed 30 days, Participant may elect to terminate the Agreement and CalMHSA shall immediately discontinue all services affected (unless the notice directs otherwise) and notify Participant as to the status of its performance. The date of termination shall be the date the notice is received by CalMHSA, unless the notice directs otherwise.
4. Payment for Services Rendered. In the event of termination by Participant for any reason whatsoever, Participant acknowledges and agrees that Participant shall be liable to CalMHSA for payment for services and/or deliverables rendered prior to the termination.
- B. By CalMHSA. Should Participant fail to pay CalMHSA all or any part of the payment set forth in EXHIBIT A, SECTION IV, CalMHSA may, at CalMHSA's option terminate this Agreement if such failure is not remedied by Participant within thirty (30) days of written notice to Participant of such late payment.
- C. Upon Termination. CalMHSA shall deliver to Participant all data, estimates, graphs, summaries, reports, and all other property, records, documents or papers intended by the Parties to be owned by Participant ("work made for hire") in the performance of this Agreement, whether completed or in process, except such items as Participant may, by written permission, permit CalMHSA to retain. Notwithstanding any other payment provision of this Agreement, Participant shall pay CalMHSA for conforming services performed to the date of termination to include a prorated amount of compensation due hereunder less payments, if any, previously made. In no event shall CalMHSA be paid an amount in excess of the full price under this Agreement nor for profit on unperformed portions of service. CalMHSA shall furnish to Participant such financial information as in the reasonable judgment of Participant is necessary to determine the reasonable value of the services rendered by CalMHSA. The foregoing is cumulative and shall not affect any right or remedy which either party may have in law or equity.

X. Miscellaneous

- A. Designated Representative. Director at phone number 805-681-5220 is the representative of Participant and will administer this Agreement for and on behalf of Participant. Ken Riomales at phone number (279) 220 3802 is the authorized representative for CalMHSA. Changes in designated representatives shall be made only after advance written notice to the other party.
- B. Notices. Any notice or consent required or permitted to be given under this Agreement shall be given to the respective Parties in writing, by personal delivery or facsimile, or with postage prepaid by first class mail, registered or certified mail, or express courier service, as follows:

To Participant: Director
 County of Santa Barbara
 Department of Behavioral Wellness

August 6, 2025

300 N. San Antonio Road
Santa Barbara, CA 93110
Fax: 805-681-5262

To CalMHSA:

Ken Riomales, Senior Director of Interoperability
CalMHSA
1610 Arden Way STE 175
Sacramento, CA, 95815
Phone: (279) 220-3802

or at such other address or to such other person that the Parties may from time to time designate in accordance with this Notices section. If sent by first class mail, notices and consents under this section shall be deemed to be received five (5) days following their deposit in the U.S. mail. This Notices section shall not be construed as meaning that either party agrees to service of process except as required by applicable law.

- C. Independent Contractor. It is mutually understood and agreed that CalMHSA (including any and all of its officers, agents, and employees), shall perform all of its services under this Agreement as an Independent Contractor as to Participant and not as an officer, agent, servant, employee, joint venturer, partner, or associate of Participant. Furthermore, Participant shall have no right to control, supervise, or direct the manner or method by which CalMHSA shall perform its work and function. However, Participant shall retain the right to administer this Agreement so as to verify that CalMHSA is performing its obligations in accordance with the terms and conditions hereof. CalMHSA understands and acknowledges that it shall not be entitled to any of the benefits of a Participant employee, including but not limited to vacation, sick leave, administrative leave, health insurance, disability insurance, retirement, unemployment insurance, workers' compensation and protection of tenure. CalMHSA shall be solely liable and responsible for providing to, or on behalf of, its employees all legally-required employee benefits. In addition, CalMHSA shall be solely responsible and save Participant harmless from all matters relating to payment of CalMHSA's employees, including compliance with Social Security withholding and all other regulations governing such matters. It is acknowledged that during the term of this Agreement, CalMHSA may be providing services to others unrelated to the Participant or to this Agreement.
- D. Standard of Performance. CalMHSA represents that it has the skills and expertise necessary to perform the services required under this Agreement. Accordingly, CalMHSA shall perform all such services in the manner and according to the standards observed by a competent practitioner of the same profession in which CalMHSA is engaged. All products of whatsoever nature, which CalMHSA delivers to Participant pursuant to this Agreement, shall conform to the standards of quality normally observed by a person practicing in CalMHSA's profession. CalMHSA shall correct or revise any material errors in the Services that are within CalMHSA's control, at Participant's request and at no additional cost, provided such errors do not arise from third-party systems,

August 6, 2025

data, or factors outside CalMHSA's reasonable control. CalMHSA shall, at its own expense, obtain and maintain any licenses required under applicable laws, regulations, or its own Joint Powers Agreement and Bylaws necessary to provide the Services under this Agreement. This does not include third-party software licenses or permits specific to Participant's systems or responsibilities.

- E. Debarment and Suspension. CalMHSA certifies to Participant that it and its employees and principals are not debarred, suspended, or otherwise excluded from, or ineligible for participation in, federal, state, or county government contracts including, but not limited to, exclusion from participation in any federal health care program under Sections 1128 or 1128A of the Social Security Act. CalMHSA certifies that it shall not contract with a subcontractor that is so debarred, suspended, excluded, or ineligible.
- F. Taxes. CalMHSA shall pay all taxes, levies, duties, and assessments of every nature due of CalMHSA in connection with any work under this Agreement and shall make any and all payroll deductions required by law. Participant shall not be responsible for paying any taxes on CalMHSA's behalf, and should Participant be required to do so by state, federal, or local taxing agencies, CalMHSA agrees to promptly reimburse Participant for the full value of such paid taxes. These taxes shall include, but not be limited to, the following: FICA (Social Security), unemployment insurance contributions, income tax, disability insurance, and workers' compensation insurance.
- G. Conflict of Interest. CalMHSA covenants that CalMHSA presently has no employment or interest and shall not acquire any employment or interest, direct or indirect, including any interest in any business, property, or source of income, which would conflict in any manner or degree with the performance of services required to be performed under this Agreement. CalMHSA further covenants that in the performance of this Agreement, no person having any such interest shall be employed by CalMHSA. CalMHSA must promptly disclose to the Participant, in writing, any potential conflict of interest. Participant retains the right to waive a conflict of interest disclosed by CalMHSA if Participant determines it to be immaterial, and such waiver is only effective if provided by Participant to CalMHSA in writing. CalMHSA acknowledges that state laws on conflict of interest apply to this Agreement including, but not limited to, the Political Reform Act of 1974 (Gov. Code, § 81000 et seq.), Public Contract Code Section 10365.5, and Government Code Section 1090.
- H. Ownership of Documents and Intellectual Property.
 - A. Participant shall be the legal owner and Custodian of Records for all Participant client files generated pursuant to this Agreement, subject to CalMHSA's rights to access and use as needed for the purposes of this Agreement.
 - B. CalMHSA warrants that any items directly provided by CalMHSA under this Agreement will not infringe upon any intellectual property or proprietary rights of any third party. CalMHSA at its own expense shall defend, indemnify, and hold harmless Participant against any claims arising solely from CalMHSA's direct infringement of third-party IP rights. CalMHSA shall pay any damages, costs, settlement amounts, and fees (including attorneys' fees) that may be incurred by Participant in connection with any such claims. This Ownership of

Documents and Intellectual Property provision shall survive expiration or termination of this Agreement.

- I. No Publicity or Endorsement. Neither party shall use the other party's name or logo or any variation of such name or logo in any publicity, advertising or promotional materials. Neither party shall use the other party's name or logo in any manner that would give the appearance that either party is endorsing the other party. Neither party shall in any way contract on behalf of or in the name of the other party. Neither party shall release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning the other party or its projects, without obtaining the prior written approval of the other party.
- J. Participant Property and Information. All of Participant's property, documents, and information provided for CalMHSA's use in connection with the services shall remain Participant's property, and CalMHSA shall return any such items whenever requested by Participant and whenever required according to the Termination section of this Agreement. CalMHSA may use such items only in connection with providing the services. CalMHSA shall not disseminate any Participant property, documents, or information without Participant's prior written consent.
- K. Records, Audit, and Review.
 1. Subject to Participant providing reasonable advance notice, CalMHSA shall make available for inspection, copying, evaluation, or audit, all of its premises; physical facilities, or such parts thereof as may be engaged in the performance of the Agreement; equipment; books; records, including but not limited to beneficiary records; prescription files; documents, working papers, reports, or other evidence; contracts; financial records and documents of account, computers; and other electronic devices, prepared in the normal course of business by CalMHSA pertaining to any aspect of services and activities performed, or determination of amounts payable, under this Agreement (hereinafter referred to as "Records"), at any time by Participant, Department of Health Care Services (DHCS), Centers for Medicare & Medicaid Services (CMS), Department of General Services, Bureau of State Audits, Health and Human Services (HHS), Inspector General, U.S. Comptroller General, or other authorized federal or state agencies, or their designees ("Authorized Representative") (hereinafter referred to as "Audit").
 2. Any such Audit shall occur at the CalMHSA's place of business, premises, or physical facilities during normal business hours, and to allow interviews of any employees who might reasonably have information related to such Records. CalMHSA shall maintain Records in accordance with the general standards applicable to such book or record keeping and shall follow accounting practices and procedures sufficient to evaluate the quality and quantity of services, accessibility and appropriateness of services, to ensure fiscal accountability, and to properly reflect all direct and indirect costs of whatever nature claimed to have been incurred in the performance of this Agreement, including any matching costs and expenses. All records must be capable of verification by qualified auditors.
 3. This Audit right will exist for 10 years from: the close of the State fiscal year in which the Agreement was in effect or if any litigation, claim, negotiation, Audit, or other action involving

August 6, 2025

- the Records has been started before the expiration of the 10-year period, the Records shall be retained until completion of the action and resolution of all issues which arise from it, or until the end of the regular 10-year period, whichever is later.
4. CalMHSA shall retain all records and documents originated or prepared by CalMHSA in the normal course of business pursuant to CalMHSA's or subcontractor's performance under this Agreement, including beneficiary grievance and appeal records identified in 42 C.F.R. § 438.416 and the data, information and documentation specified in 42 Code of Federal Regulations Sections 438.604, 438.606, 438.608, and 438.610 for the 10-year period as determined in Section X.K (Records, Audit, and Review).
 5. If this Agreement is completely or partially terminated, the Records, relating to the work terminated shall be preserved and made available for the 10-year period as determined in Section X.K (Records, Audit, and Review).
 6. CalMHSA may, at its discretion, following receipt of final payment under this Agreement, reduce its accounts, books and records related to this Agreement to microfilm, computer disk, CD ROM, DVD, or other data storage medium. Upon request by an Authorized Representative to inspect, audit or obtain copies of said records, CalMHSA must supply or make available applicable devices, hardware, and/or software necessary to view, copy and/or print said records. Applicable devices may include, but are not limited to, microfilm readers and microfilm printers, etc.
 7. The Authorized Representatives may Audit CalMHSA at any time if there is a reasonable possibility of fraud or similar risk.
 8. CalMHSA agrees to include a similar right of Authorized Representatives to audit records and interview staff in any subcontract related to performance of this Agreement.
 9. If federal, state or County audit exceptions are made relating to this Agreement, CalMHSA shall reimburse all reasonable costs incurred by federal, state, and/or County governments associated with defending against the audit exceptions or performing any audits or follow-up audits, including but not limited to: audit fees, court costs, attorneys' fees based upon a reasonable hourly amount for attorneys in the community, travel costs, penalty assessments and all other costs of whatever nature. Immediately upon notification from Participant, CalMHSA shall reimburse the amount of the audit exceptions and any other related costs directly to Participant as specified by Participant in the notification. The provisions of the Records, Audit, and Review section shall survive any expiration or termination of this Agreement.
- L. Nondiscrimination and Compliance (GTC 02/2025).
1. During the performance of this Agreement, CalMHSA shall not deny this Agreement's benefits to any person on the basis of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status, nor shall they discriminate unlawfully against any employee or applicant for employment because of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex,

August 6, 2025

gender, gender identity, gender expression, age, sexual orientation, or military and veteran status. CalMHSA shall ensure that the evaluation and treatment of employees and applicants for employment are free of such discrimination. CalMHSA shall comply with the provisions of the California Fair Employment and Housing Act (Gov. Code, § 12900 et seq.), the regulations promulgated thereunder (2 C.C.R. § 11000 et seq.), the provisions of article 9.5, chapter 1, part 1, division 3, title 2 of the Government Code (Gov. Code, §§ 11135–11139.5), and the regulations or standards adopted by the California Department of Health Care Services (DHCS) to implement such article. CalMHSA shall permit access by representatives of the California Civil Rights Department (CRD) and DHCS upon reasonable notice at any time during normal business hours, but in no case less than 24 hours' notice, to such of its books, records, accounts, and all other sources of information and its facilities as CRD or DHCS shall require to ascertain compliance with this provision. CalMHSA shall give written notice of their obligations under this provision to labor organizations with which they have a collective bargaining or other agreement. (See Cal. Code Regs., tit. 2, § 11105.)

- M. **Nonexclusive Agreement.** CalMHSA understands that this is not an exclusive Agreement and that Participant shall have the right to negotiate with and enter into contracts with others providing the same or similar services as those provided by CalMHSA as the Participant desires. Should Participant enter into such negotiations, Participant agrees to keep confidential and not disclose any and all information of CalMHSA's which, by its nature, is confidential, proprietary, non-public, or should reasonably be kept confidential ("Confidential Information"). Participant further agrees to exercise the same degree of care with CalMHSA's Confidential Information which it would exercise with its own confidential, proprietary or non-public information.
- N. **Nonassignment.** CalMHSA shall not assign or transfer this Agreement or any of its rights or obligations under this Agreement without the prior written consent of Participant and any attempt to so assign or transfer without such consent shall be void and without legal effect and shall constitute grounds for termination.
- O. **Subcontractors.** CalMHSA shall require its subcontractors to comply with all Program requirements in the delivery of services under this Participation Agreement to the extent such requirements pertain to the subcontractor's performance under this Agreement.
- P. **Section Headings.** The headings of the several sections, and any Table of Contents appended hereto, shall be solely for convenience of reference and shall not affect the meaning, construction or effect hereof.
- Q. **Severability.** If any one or more of the provisions contained herein shall for any reason be held to be invalid, illegal or unenforceable in any respect, then such provision or provisions shall be deemed severable from the remaining provisions hereof, and such invalidity, illegality or unenforceability shall not affect any other provision hereof, and this Agreement shall be construed as if such invalid, illegal or unenforceable provision had never been contained herein.
- R. **No Waiver or Default.** No delay or omission of Participant to exercise any right or power arising upon the occurrence of any event of default shall impair any such right or power or shall be construed to be a waiver of any such default or an acquiescence therein.

- S. Entire Agreement and Amendment. In conjunction with the matters considered herein, this Agreement contains the entire understanding and agreement of the Parties and there have been no promises, representations, agreements, warranties or undertakings by any of the Parties, either oral or written, of any character or nature hereafter binding except as set forth herein. This Agreement may be altered, amended or modified only by an instrument in writing, executed by the Parties to this Agreement and by no other means. Each party waives their future right to claim, contest or assert that this Agreement was modified, canceled, superseded, or changed by any oral agreements, course of conduct, waiver or estoppel. All requests for changes shall be in writing. Changes shall be made by an amendment pursuant to this section. Any amendments or modifications that do not materially change the terms of this Agreement (such as changes to the Designated Representative or CalMHSA's address for purposes of Notice) may be approved by the Director of the Department of Behavioral Wellness or designee. Except as otherwise provided in this Agreement, the Board of Supervisors of the County of Santa Barbara must approve all other amendments and modifications.
- T. Successors and Assigns. All representations, covenants and warranties set forth in this Agreement, by or on behalf of, or for the benefit of any or all of the Parties hereto, shall be binding upon and inure to the benefit of such party, its successors and assigns.
- U. Compliance with Law. CalMHSA shall, at its sole cost and expense, comply with all State and Federal ordinances; statutes; regulations; orders including, but not limited to, executive orders, court orders, and health officer orders; policies; guidance; bulletins; information notices; and letters including, but not limited to, those issued by the California Department of Health Care Services (DHCS) now in force or which may hereafter be in force with regard to this Agreement. The judgment of any court of competent jurisdiction, or the admission of CalMHSA in any action or proceeding against CalMHSA, whether Participant is a party thereto or not, that CalMHSA has violated any such ordinance, statute, regulation, order, policy, guidance, bulletin, information notice, and/or letter shall be conclusive of that fact as between CalMHSA and Participant.
- V. California Law and Jurisdiction. This Agreement shall be governed by the laws of the State of California. Any litigation regarding this Agreement or its contents shall be filed in the County of Santa Barbara, if in state court, or in the federal district court nearest to Santa Barbara County, if in federal court.
- W. Survival. All provisions of this Agreement which by their nature are intended to survive the termination or expiration of this Agreement shall survive such termination or expiration.

THIS SECTION LEFT BLANK INTENTIONALLY

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. "Health Information Exchange" or "HIE" shall have the same meaning as "health information exchange" as set forth in the Federal Information Blocking Regulations (45 C.F.R. § 171.102).
- L. "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.
- M. "Individual User" shall mean the person who is the subject of PHI or PII.
- N. "Payment" shall have the same meaning as set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.

- O. "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.
- P. "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).
- Q. "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.
- R. "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.
- 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. "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.
- V. "Social Services Activities" shall mean the Social Services provided by Social Service Organizations.
- W. "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.
- X. "Submitter" shall mean a Party that submits PHI, PII or other data to a Recipient.
- Y. "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.

- Z. "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. Consistent with Health and Safety Code § 130290(b) and applicable law, Parties are not required to exchange abortion or abortion-related services information as part of the exchange and/or access required by this section 4.A.
- 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 knowledgeable 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. The Party shall issue a Breach notification promptly once law enforcement determines the notification will not impede a criminal investigation.

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, 42 C.F.R. Part 2, the California Consumer Privacy Act, the California Confidentiality of Medical Information Act, the Information Practices Act, the Lanterman-Petris-Short Act, the Lanterman Developmental Disabilities Services Act, and California Health and Safety Code § 11845.5. The Parties shall only exchange abortion or abortion-related services information or gender affirming care information in compliance with Applicable Law.
- 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. SECURE DESTRUCTION. In the event a Party discovers that it has received PHI, PII or other data about an Individual in error, the receiving Party must, as soon as practicable, Securely Destroy the information and notify the Party that erroneously Disclosed the information. In addition, all Parties shall comply with any obligations they may have under Section 6, Breach Notification of this Data Sharing Agreement and any Applicable Law.

- D. 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, California Health and Safety Code § 11845.5, California Lanterman-Petris-Short Act (see Cal. Welf. & Inst. Code § 5328 et seq.), Lanterman Developmental Disabilities Services Act (see Cal. Welf. & Inst. Code § 4514 et seq.), and to the extent applicable to outpatient behavioral health information, the California Confidentiality of Medical Information Act (see Cal. Civ. Code § 56 et seq.)
- E. 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 faith to implement the provisions of this Agreement. The Parties agree to provide such non-privileged information to each other Party as reasonably requested for purposes of performing activities related to this Agreement and the underlying Participation Agreement. The Parties agree to actively engage in the bilateral or multilateral exchange of information with the other Party as both a Submitter and Recipient of information to the extent permitted or required under this Agreement and Applicable Law. The Parties agree to devote such time as may be reasonably requested to review information, meet with, respond to, and advise the other Party with respect to activities as they relate to this 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. The Parties agree that in seeking the other Party's cooperation, each Party shall make all reasonable efforts to accommodate the other Party's schedules and reasonable operational concerns.

12. INFORMATION BLOCKING

Parties shall not engage in Information Blocking, as set forth in the Federal Information Blocking Regulations (45 C.F.R. Part 171, as may be amended), for PHI, PII or other data Accessed, Used, or Exchanged for a Required Purpose. Parties shall be considered in compliance if they comply with the Federal Information Blocking Regulations. Parties may also rely on current and future guidance from the federal government to interpret the requirements of the Federal Information Blocking Regulations. When the Federal Information Blocking Regulations use the term "electronic health information," the term PHI, PII, and other data shall also apply.

13. 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.

14. 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.

15. 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.

16. 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.

17. TERM

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

18. 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.

19. 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.

20. 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.

21. 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.

22. SURVIVAL

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

23. 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.

24. 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.

25. 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.

THIS SECTION LEFT BLANK INTENTIONALLY

Agreement No. 5127-ARCHIVE-2023-SB

Data Archive Solution

August 6, 2025

EXHIBIT BAA
HIPAA BUSINESS ASSOCIATE
AGREEMENT

Agreement No. 5127-ARCHIVE-2023-SB
Data Archive Solution
August 6, 2025



County of Santa Barbara

BOARD OF SUPERVISORS

Minute Order

September 13, 2022

Present: 5 - Supervisor Williams, Supervisor Hart, Supervisor Hartmann, Supervisor Nelson, and Supervisor Lavagnino

BEHAVIORAL WELLNESS DEPARTMENT

File Reference No. 22-00816

RE: Consider recommendations regarding the California Mental Health Services Authority (CalMHSA) Behavioral Health Quality Improvement Program (BHQIP) Participation Agreement, Fiscal Years (FYs) 2022-2024, Psychiatric Inpatient Concurrent Review (PICR) Participation Agreement, FYs 2022-2025 and Business Associates Agreement under the Health Insurance Portability and Accountability Act of 1996 (BAA), as follows:

a) Approve and authorize the Chair to execute the CalMHSA BHQIP Participation Agreement No. 1303-BHQIP-2022-SB to procure consultation services for the development, implementation, and continued support of the County's Behavioral Health Plan to meet milestones required to complete the California Department of Health Care Services (DHCS) California Advancing and Innovating Medi-Cal (CalAIM) BHQIP mandated deliverables, for a maximum agreement amount not to exceed \$22,080.00 from the date of execution by the County through June 30, 2024;

b) Approve and authorize the Chair to execute the CalMHSA PICR Participation Agreement No. 1158-PICR-2022-SB to conduct concurrent review and authorization of services for all psychiatric inpatient hospitals and psychiatric health facilities where the County client is placed, for a Maximum Agreement Amount not to exceed \$178,483.20 inclusive of a \$6,374.40 administrative fee, from the date of execution by the County through December 31, 2024;

c) Approve and authorize the Chair to execute a Business Associates Agreement under the Health Insurance Portability and Accountability Act of 1996 (BAA) with CalMHSA to allow for the exchange of private health information (PHI) and personal identifiable information (PII) as it applies to all Participation Agreements between the County and CalMHSA, as required and necessary to perform DHCS-mandated services, which are to begin upon execution of the BAA Agreement; and

d) Determine that the above actions are government funding mechanisms or other government fiscal activities, which do not involve any commitment to any specific project that may result in a potentially significant physical impact on the environment, and are organizational or administrative



County of Santa Barbara

BOARD OF SUPERVISORS

Minute Order

September 13, 2022

activities of the government that will not result in direct or indirect physical changes in the environment and are therefore not a project under the California Environmental Quality Act (CEQA) pursuant to section 15378(b)(4) and (b)(5) of the CEQA Guidelines.

A motion was made by Supervisor Nelson, seconded by Supervisor Lavagnino, that this matter be acted on as follows:

a) through c) Approved and authorized; Chair to execute; and

d) Approved.

The motion carried by the following vote:

Ayes: 5 - Supervisor Williams, Supervisor Hart, Supervisor Hartmann, Supervisor Nelson, and Supervisor Lavagnino



BOARD OF SUPERVISORS AGENDA LETTER

Agenda Number:

Clerk of the Board of Supervisors
105 E. Anapamu Street, Suite 407
Santa Barbara, CA 93101
(805) 568-2240

Department Name: Behavioral Wellness
Department No.: 043
For Agenda Of: September 13, 2022
Placement: Administrative
Estimated Time: N/A
Continued Item: No
If Yes, date from:
Vote Required: Majority

TO: Board of Supervisors

FROM: Department Antonette Navarro, LMFT, Director
Director(s) Department of Behavioral Wellness, (805) 681-5220
Contact Info: Jamie Huthsing, Division Chief of Quality Care Management,
Department of Behavioral Wellness, (805) 681-5220
Celeste Andersen, Chief of Compliance, Department of
Behavioral Wellness, (805) 681-5220

SUBJECT: Behavioral Wellness - California Mental Health Services Authority (CalMHSA) Behavioral Health Quality Improvement Program (BHQIP) Participation Agreement Fiscal Year (FY) 2022-2024, Psychiatric Inpatient Concurrent Review (PICR) Participation Agreement FY 2022-2025 and Business Associates Agreement under the Health Insurance Portability and Accountability Act of 1996 (BAA)

County Counsel Concurrence

As to form: Yes

Other Concurrence: Risk Management

As to form: Yes

Auditor-Controller Concurrence

As to form: Yes

Recommended Actions:

That the Board of Supervisors:

- A. Approve and authorize the Chair to execute the **California Mental Health Services Authority (CalMHSA) Behavioral Health Quality Improvement Program (BHQIP) Participation Agreement No. 1303-BHQIP-2022-SB** to procure consultation services for the development, implementation, and continued support of the County's Behavioral Health Plan to meet milestones required to complete the California Department of Health Care Services (DHCS) California Advancing and Innovating Medi-Cal (CalAIM) BHQIP mandated deliverables, for a Maximum Agreement Amount not to exceed **\$22,080** from the date of execution by the County through June 30, 2024 (Attachment A);

- B. Approve and authorize the Chair to execute the **California Mental Health Services Authority (CalMHSA) Psychiatric Inpatient Concurrent Review (PICR) Participation Agreement No. 1158-PICR-2022-SB** to conduct concurrent review and authorization of services for all psychiatric inpatient hospitals and psychiatric health facilities where the County client is placed, for a Maximum Agreement Amount not to exceed **\$178,483.20** inclusive of a \$6,374.40 administrative fee, from the date of execution by the County through December 31, 2024 (Attachment B);
- C. Approve and authorize the Chair to execute a **Business Associates Agreement under the Health Insurance Portability and Accountability Act of 1996 (BAA)** with **California Mental Health Services Authority (CalMHSA)** to allow for the exchange of private health information (PHI) and personal identifiable information (PII) as it applies to all Participation Agreements between the County and CalMHSA, as required and necessary to perform DHCS-mandated services, which are to begin upon execution of the BAA Agreement (Attachment C); and
- D. Determine that the above actions are government funding mechanisms or other government fiscal activities, which do not involve any commitment to any specific project that may result in a potentially significant physical impact on the environment, and are organizational or administrative activities of the government that will not result in direct or indirect physical changes in the environment and are therefore not a project under the California Environmental Quality Act (CEQA) pursuant to section 15378(b)(4) and (b)(5) of the CEQA Guidelines.

Summary Text:

The above-referenced items are on the agenda to request the Board of Supervisors (Board) to approve and authorize the Chair to execute agreements with CalMHSA, BHQIP Participation Agreement No. 1303-BHQIP-2022-SB for the procurement of consultation services for the development, implementation, and continued support of the County's Behavioral Health Plan to meet the milestones required to complete the CalAIM BHQIP deliverables for an amount of \$22,080 from the date of execution through June 30, 2024, and PICR Participation Agreement No. 1158-PICR-2022-SB to conduct concurrent review and authorization of services for all psychiatric inpatient hospital and psychiatric health facilities in the County for a Maximum Agreement Amount not to exceed \$178,483.20, from the date of execution through December 31, 2024. Also, the Department of Behavioral Wellness (BWell) requests the Board to approve and authorize the Chair to execute a BAA with CalMHSA to allow for the exchange of PHI and PII, as it applies to all Participation Agreements between the County and CalMHSA, as required and necessary to perform DHCS-mandated services upon execution of the Agreement.

Background:

The California Government Code ("Joint Exercise of Powers Act," Section 6500 et seq.) permits two or more public agencies to jointly exercise powers common to the contracting parties through an agreement. CalMHSA is a Joint Powers Authority (JPA) formed in 2009 for the purpose of creating a separate public entity to provide administrative and fiscal services in support of its members. CalMHSA assists its members with the operation of various programs to contract and/or negotiate with the State or other providers; contract and/or negotiate with the State or Federal government for administration of mental health services, programs or activities, including managed mental health care and the delivery of specialty mental health services.

They also provide fiscal or administrative services to its members such as group purchasing, contract management, research and development, data management, maintenance of a research depository, technical assistance, capacity building, education, and training; and execution of policy requests. CalMHSA also provides its members with the ability to deal jointly with the California Department of Health Care Services (DHCS), Department of State Hospitals (DSH), the Mental Health Services Oversight and Accountability Commission (MHSOAC), and the legislature.

In 2014, the Board approved Behavioral Wellness' membership in CalMHSA. BWell currently has five agreements with CalMHSA--to deliver services for loan repayment, state hospital beds, Tech Suite, Help@Hand, and payment of Presumptive Transfer, all of which were previously approved by the Board.

BHQIP: Under CalAIM, BHQIP is an incentive payment program to support Mental Health Plans (MHP), Drug Medi-Cal State Plans (DMC), and Drug Medi-Cal Organized Delivery Systems (DMC-ODS), as they prepare for changes in the CalAIM initiative and other approved administration priorities. CalAIM is a DHCS initiative to reform the Medi-Cal program to help address many of the complex challenges facing California's most vulnerable residents. It offers beneficiaries a more equitable, coordinated, person-centered approach to maximize their health. The BHQIP priorities/milestones include payment reform, behavioral health policy changes, and bi-directional data exchange between systems of care for the purpose of improving quality and behavioral health outcomes and care coordination for Medi-Cal beneficiaries. Each participating entity earns incentive payments in the CalAIM BHQIP by achieving these milestones.

CalMHSA will provide BWell with assistance to achieve the Policy Change Milestone to update Utilization Management Protocols by conducting a landscape analysis of documentation audit practices and draft an updated Utilization Management protocol to comply with best practices and updated documentation audit standards. In addition, in order to achieve the Data Exchange Milestone, CalMHSA will collect and analyze Managed Care Plan (MCP) data to establish baseline performance on Follow-up After Emergency Department Visit for Alcohol and Other Drug Abuse or Dependence (FUA), Follow-up After Emergency Department Visit for Mental Illness (FUM), and Pharmacotherapy for Opioid Use Disorder (POD).

PIRC: DHCS state and federal regulations require County Mental Health Plan (MHP) Specialty Mental Services (SMHS) and Substance Use Disorder Services (SUDS) authorization of specialty health services. To ensure compliance with Parity in Mental Health and Substance Use Disorder Services Final Rule (Parity Rule; Title 42 of the C.F.R., § 438.910), DHCS Behavioral Health Information Notice (BHIN) 19-026 requires MHPs to operate a utilization management (UM) program that ensures beneficiaries have appropriate access to SMHS. MHPs are required to conduct concurrent review and authorization for all psychiatric inpatient hospital services and psychiatric health facility services. MHPs shall conduct concurrent review of treatment authorizations following the first day of admission. The County will incur a \$6,374.40 administrative fee, which is included in the total cost of the program.

CalMHSA has entered into a services agreement with Keystone Peer Review Organization, Inc. (Kepro), who shall conduct concurrent review and authorization of inpatient psychiatric hospital services on behalf of multiple California County MHPs. By utilizing Kepro's technology-assisted concurrent review process, CalMHSA will ensure a consistent and efficient review process across participating counties and will support MHP compliance with DHCS BHIN 19-026 and the Parity Rule.

BAA: The addition of the JPA BAA with CalMHSA will allow BWell to share clients' private PHI and PII for our current or future project/programs with CalMHSA that are necessary for the delivery of SMHS mandated services and will support payment reform and the development of new Medi-Cal rates under CalAIM, which is set to launch in 2023. Both the BHQIP and the PIRC programs require the exchange of PHI/PII to comply with DHCS compliance requirements. Under the BHQIP agreement, CalMHSA will need to collect and analyze BWell client data to establish baseline performance on FUA/FUM/POD. Under CalMHSA PICR, through their contract with Kepro, CalMHSA will need access to Psychiatric Hospital client information to conduct web based concurrent review to comply with state and federal regulations and for Medi-Cal reimbursement.

The approval of the recommend actions would streamline the payment and billing process for Medi-Cal services.

Performance Measure:

CalMHSA facilitates the efficient use of resources for multiple public entities by providing group purchasing power, joint development of Requests for Proposal (RFPs) and contracts for services, reduced overhead costs through sharing of the expenses of administration and reporting, and shared research and strategies. CalMHSA's administration of this program will result in greater efficiency in the implementation of these mandated services for compliance with state and federal requirements.

Fiscal and Facilities Impacts:

Budgeted: Yes

Fiscal Analysis:

<u>Funding Sources</u>	<u>BHQIP Cost FY 22-24</u>
General Fund	
State	\$ 11,040.00
Federal	\$ 11,040.00
Fees	
Other:	
Total	\$ 22,080.00

<u>Funding Sources</u>	<u>PIRC Cost FY 22-23</u>	<u>Cost FY 23-24</u>	<u>Cost through 12/31/2024 FY 24-25</u>
General Fund			
State	\$ 35,696.64	\$ 35,696.64	\$ 17,848.32
Federal	\$ 35,696.64	\$ 35,696.64	\$ 17,848.32
Other:			
Total	\$ 71,393.28	\$ 71,393.28	\$ 35,696.64
Grand Total			\$ 178,483.20

Narrative:

Key Contract Risks:

The County may withdraw from the Program upon six months' written notice to CalMHSA.

Page 5 of 5

Special Instructions:

Please return one (1) Minute Order and one (1) complete copy of the above items to Denise Morales at dmorales@sbcbswell.org and the BWell Contracts Division at bwellcontractsstaff@sbcbswell.org.

Attachments:

Attachment A: CalMHSA FY 22-24 PA No. 1303-BHQIP-2022-SB

Attachment B: CalMHSA FY 22-25 PA No. 1158-PICR-2022-SB

Attachment C: CalMHSA Agreement No. 1327-BAA-2022-SB

Authored by:

D. Morales

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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

Santa Barbara 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 "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.

Agreement No. 1327-BAA-2022-SB
 Santa Barbara County
 August 30, 2022

- 1.3 "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 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).
- 1.4 "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.
- 1.5 "Data Aggregation" has the same meaning as the term "data aggregation" at 45 C.F.R. § 164.501.
- 1.6 "De-identification" refers to the de-identification standard at 45 C.F.R. § 164.514.
- 1.7 "Designated Record Set" has the same meaning as the term "designated record set" at 45 C.F.R. § 164.501.
- 1.8 "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.)
- 1.9 "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.)
- 1.10 "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.
- 1.11 "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.
- 1.12 "Health Care Operations" has the same meaning as the term "health care operations" at 45 C.F.R. § 164.501.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- 1.13 "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).
- 1.14 "Law Enforcement Official" has the same meaning as the term "law enforcement official" at 45 C.F.R. § 164.103.
- 1.15 "Minimum Necessary" refers to the minimum necessary standard at 45 C.F.R. § 164.502(b).
- 1.16 "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.
- 1.17 "Required by Law" " has the same meaning as the term "required by law" at 45 C.F.R. § 164.103.
- 1.18 "Secretary" has the same meaning as the term "secretary" at 45 C.F.R. § 160.103.
- 1.19 "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, Participation Agreement, 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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 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, 2.6 and 2.7.
- 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

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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 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 number 1-805-934-6344 (Privacy Line)** 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;

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- (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 Privacy Officer at: Janet Alexander, LMFT

County/Department: Santa Barbara County Department of Behavioral Wellness, Quality Care Management/Access Team

Address: 300 N. San Antonio Road, Santa Barbara, CA 93110

Email: jalexander@sbcbswell.org or BWellPrivacy@sbcbswell.org,

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;

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- (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 law enforcement official states to Business Associate that notification would impede a criminal investigation or cause damage to national security.

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.

Agreement No. 1327-BAA-2022-SB
 Santa Barbara County
 August 30, 2022

- 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, the 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

- 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

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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;
- (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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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 applicable Privacy and Security Regulations, including the HIPAA rules.
- 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.
- 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;

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- (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. INDEMNIFICATION

- 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 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.

Agreement No. 1327-BAA-2022-SB
 Santa Barbara County
 August 30, 2022

- 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, 2.6, and 2.7.

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 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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, if agreed to by Covered entity, 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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 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, 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, 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, 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.
- 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- 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, 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, the provision of this Business Associate Agreement shall control. Otherwise, this Business Associate Agreement shall be construed under, and in accordance with, the terms of the applicable underlying Agreement, Contract, Participation Agreement, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without
- 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 Contractor that require Contractor to create, access, receive, maintain, and/or transmit protected health information or personally identifiable information.

AUTHORIZED SIGNORS:

CONTRACTOR: CALIFORNIA MENTAL HEALTH SERVICES AUTHORITY (CalMHSA)

Signed: DocuSigned by: Amie Miller Name (Printed): Amie Miller, Psy.D., MFT
82E9EFB8B7CC446...
Title: Executive Director Date: 8/31/2022
Address: 1610 Arden Way, Suite 175, Sacramento, CA 95815 Phone: (279) 234-0700
Email: amie.miller@calmhhsa.org

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

COUNTY OF SANTA BARBARA:

Signed: 

Name: Joan Hartmann

Title: Chair, Board of Supervisors

Date: 9-13-22

ATTEST:

Signed: 

Name: Mona Miyasato

Title: County Executive Officer, Clerk of the Board

Date: 9-13-22

RECOMMENDED FOR APPROVAL:

Signed: 

Name: Antonette Navarro, LMFT

Title: Director, Behavioral Wellness

Date: 8/31/2022

APPROVE AS TO FORM: COUNTY COUNSEL

Signed: 

Name: Bo Bae

Title: Deputy County Counsel

Date: 9/1/2022

APPROVE AS TO ACCOUNTING FORM: AUDITOR-CONTROLLER

Signed: 

Name: C. Edwin Price, Jr.

Title: Deputy

Date: 9/1/2022

APPROVE AS TO INSURANCE FORM: RISK MANAGEMENT:

Signed: 

Name: Greg Milligan

Title: Risk Manager

Date: 8/31/2022

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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, even if except if disclosure is required by State or Federal law.
6. Business Associate shall observe the following requirements:
 - 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 PI. 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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.
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 PI. 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)

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- 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.
 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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 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.

Agreement No. 1327-BAA-2022-SB
 Santa Barbara County
 August 30, 2022

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 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 (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Use" near the middle of the page) or use this link: <http://www.dhcs.ca.gov/formsandpolicies/laws/priv/Policies/DHCSBusinessAssociatesOnline.aspx>
- 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- 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 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

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- 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 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- 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 PI. These steps shall include, at a minimum:
 - i. Complying with all of the data system security precautions listed in Attachment A, Business 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- 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 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 (www.dhcs.camov), then select "Privacy" in the left column and then "Business Partner" near the middle of the page) or use this link: <http://www.dhcs.ca.gov/formsandoubs/laws/oriv/Paces/DHCSBusinessAssociatesOnly.aspx>.
 - 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- 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.
- 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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 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 Business Associate 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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 164.504(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 and 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

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 PI. 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- 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 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 PI. 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- 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 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.
- 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.
- 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.

Agreement No. 1327-BAA-2022-SB
Santa Barbara County
August 30, 2022

- b. **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 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 cross cut shredding and pulverizing.
- 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.