Contract Name
Program
_____, 2024

CALIFORNIA MENTAL HEALTH SERVICES AUTHORITY
"CalMHSA"
STANDARD SERVICES AGREEMENT

This Agreement is a contract by and between the California Mental Health Services Authority ("CalMHSA") and_____("Contractor") (Each may be defined as "party" or "parties" to this Agreement.

CalMHSA desires to obtain certain services from the Contractor ("Services") which are more fully described in Section 1 of this Agreement ("Scope of Work"). Contractor represents that it is willing, able to, and has sufficient experience and expertise to provide such Services to CalMHSA.

CalMHSA agrees to retain Contractor to provide the Services, and Contractor accepts such engagement, on the terms of this Agreement including any Exhibits (which Exhibits form part of this Agreement):

Check all that apply and attach same to the Agreement:

- ☑ Exhibit A – Funding Allocation Form
- ☑ Exhibit B – Privacy and Data Security Policy

Agreement Term: _____through _____

Total Funding Amount *(Up to but Not to Exceed)*: [insert]

Contractor:

Signed:_____ Name (printed):_____
Title:_____ Date:_____
Address:_____
Phone:_____ Email:_____

CalMHSA

Signed:_____ Name (printed): Dr. Amie Miller, Psy.D., MFT
Title: Executive Director Date:_____
Address: 1610 Arden Way, Suite 175,
Sacramento, CA 95815
Phone: 888-210-2515 Email: amie.miller@calmhsa.org

STANDARD SERVICES AGREEMENT

1. SCOPE OF WORK. The activities outlined in the Scope of Work set out the Services to be performed by the Contractor to support CalMHSA for [insert program or project name] ("Program"). The Scope of Work and deliverables can be adjusted with the needs of the Program as agreed upon by Contractor and CalMHSA. All changes to the Scope of Work must take place in writing via an Agreement Amendment.

Overview of Project/Services to Be Performed

[Insert summary of project and what high-level contractor is doing for CalMHSA]

Scope of Work and Deliverables

Contractor is to provide the following Services and Deliverables:

[insert deliverables/scope of work]

a)

b)

c)

d)

e)

...

☐ **Check this box if Services includes any professional or advisory services, or if the Contractor or any of its employees, consultants or CalMHSA approved subcontractor personnel who will be providing any of the Services or any part thereof are professionals or licensed in their field (e.g. MD, attorney, engineer, accountant, agency licensed, etc.) or will provide technology and/or development work. If this box is checked, Contractor must provide a Certificate of Insurance including coverage for Professional Liability for each year of the Term and for four (4) years post termination or expiry of this Agreement (see Insurance Section 6 for Insurance Coverage Requirements).**

Timelines:

Reports:

Meetings:

Location:

CalMHSA shall provide: ...

2. AGREEMENT REPRESENTATIVES. The CalMHSA representative for the performance of the Services will be [Name, Title, email, phone]: . The representative for the Contractor will be [Name, Title, Email Phone:]. Contractor will report to [Name & Title, Email, Phone].

3. TERM OF CONTRACT. This Agreement shall be effective on [insert as shown on cover page], through _____. This Agreement may be extended upon written agreement of both parties.

4. FUNDING AND FUND AVAILABILITY

4.1 **Funding and Fund Availability**: Maximum payments by CalMHSA to Contractor under this Agreement shall not exceed the amount stated in Section 5, including all expenses. CalMHSA is not responsible for any fees or costs incurred above the contracted amount and shall have no obligation to purchase any specified amount of services or products. This Agreement is subject to fund availability for the Program and is valid and enforceable only if sufficient funds are available for the purposes of this Program. This Agreement is also subject to any additional restriction, limitations or conditions enacted by one or more member counties of CalMHSA ("County Members"), which may affect the provisions, terms, or funding of this Agreement in any manner. If it is determined funds are not available or become unavailable, CalMHSA reserves the right to terminate the Agreement without penalty. Notification of such action will be issued to the Contractor no later than thirty (30) calendar days after CalMHSA has made such funding determination.

4.2 **Funding Allocation**: CalMHSA may reduce, revise, or terminate deliverables, including retroactively, which may impact the funding amount and or funding allocation per deliverable. Funding allocation changes made by CalMHSA shall not require an Agreement amendment unless such changes increase the full Agreement amount. All funding allocation changes are effective upon written notification by CalMHSA.

5. COMPENSATION, BILLING AND PAYMENT

5.1 **Compensation:** Contractor shall be compensated as set out in Exhibit E which represents full compensation for all Services and shall be inclusive of all of Contractor's out-of-pocket expenses incurred in the performance of this Agreement, including travel, unless otherwise agreed to herein.

5.2 **Budget for Hourly Services**: If CalMHSA and Contractor agree that Contractor shall be compensated on an hourly basis, Contractor shall submit a written budget to CalMHSA prior to the provision of any of

the Services for CalMHSA's approval. If Contractor reasonably anticipates that hours billed to CalMHSA may exceed Contractor's budget, Contractor must promptly notify CalMHSA and obtain CalMHSA's written approval to amend the budget. CalMHSA will not be responsible for payments to Contractor above the existing budget if Contractor does not receive CalMHSA approval for any amended budget. Contractor budget changes require an Agreement Amendment pursuant to Section 17 below.

5.3 **Invoices**: Contractor shall submit its invoice to CalMHSA monthly by the 15th of each month for work performed or deliverables met in the previous month. Contractor shall submit its final invoice within fifteen (15) business days from the final deliverable completion/acceptance date. Invoices received outside of these provisions are subject to non-payment. Contractor shall submit the original invoice to accounting as follows:

A. Email to: accountspayable@calmhsa.org
B. Each invoice shall contain the following information, at a minimum: Contractor name, invoice number and date; remittance address and phone number; the service month; Agreement account number (provided by CalMHSA); description of completed deliverable; deliverable fee charged; an invoice total; and any additional information required by CalMHSA.
C. Invoices shall be rendered in arrears.

5.4 **Payment**: CalMHSA shall pay within thirty (30) business days from the date of receipt of a satisfactory invoice, subject to the conditions of this Section 5 and compliance with the Agreement. Deliverables will be paid only upon completion, and not in fractions of the total funding allocation. Payment shall be made to Contractor only after services have been rendered or delivery of materials or products, and acceptance has been made by CalMHSA according to CalMHSA's policy for assessing deliverable completion.

5.5 **Withholding**: CalMHSA may delay or withhold any monetary payments due to the Contractor for any of the following reasons (in addition to any other remedies available at law or under this Agreement):a) Payment may be reduced, delayed, or withheld at the discretion of CalMHSA due to contract non-compliance, including failure to meet Service requirements or any deliverables in full and/or on a timely basis; b) CalMHSA will conduct a settlement under this Agreement based on an assessment of completion level of all Services and Deliverables and compliance with the Agreement, the results of which may result in offsets of the remaining amount to be paid.

6. INSURANCE. Contractor and its CalMHSA authorized subcontractors utilized on this Agreement shall purchase and maintain policies of insurance with an insurer or insurers. If Contractor has any employees or offices in the State of California, its insurers must be admitted in the State of California, and with a current A.M. Best's rating of no less than A-. If Contractor subcontracts any portion of Contractor's duties, Contractor shall require any such subcontractor to purchase and maintain insurance coverage as provided below. If Contractor is a California public entity, Contractor may satisfy the below requirements through commercial insurance or through self-insurance. Insurance shall include:

A. If Contractor has employees, Contractor shall carry workers' compensation insurance per the laws of the State of California (or the laws of the State in which the employees perform their work), and such insurance shall waive subrogation against CalMHSA.
B. Contractor shall carry automobile liability insurance including coverage for owned and hired vehicles. For non-owned vehicles, employees, consultants of Contractors and any subcontractors must be required to carry their own insurance. Such insurance is required should Contractor, its employee, consultants, or its subcontractor use a vehicle in the performance of any of the Services under this Agreement.
C. Contractor shall also carry commercial general liability insurance with coverage for liability assumed by contract. Such policies shall have limits of not less than $1,000,000 per accident or occurrence. In the event this Agreement is for a total amount of $5,000,000 or more, such policies shall have limits of at least $2,000,000 per accident or occurrence.
D. If applicable (i.e., **Contractor or its employees, contractors or subcontractors are providing professional services, advisory services, are professionals or licensed in their field or are providing technology/development work**), Contractor shall carry professional liability insurance applicable to wrongful acts, errors or omissions that may cause financial loss to CalMHSA, including contractual liability, with limits of at least $1,000,000 per claim, or at least $2,000,000 per claim if the total amount of this Agreement exceeds $5,000,000. Such insurance shall be maintained during the term of this Agreement and renewed for a period of at least four years thereafter. Contractor must provide its and its subcontractors' professional liability insurance coverage certificate each year or when asked by CalMHSA.
E. If Contractor has employees with access to CalMHSA funds or financial accounts, Contractor shall maintain a commercial crime (fidelity) policy with third-party property and employee dishonesty coverage with a minimum limit of $1,000,000.
F. Each policy of insurance required in Subsection C shall name CalMHSA and its agents, officers, governing board, and employees as additional insureds; shall state that, with respect to the operations of Contractor hereunder, such policy is primary and any insurance carried by CalMHSA or its agents, officers, governing board or employees is excess and non-contributory with such primary insurance; shall state that not less than thirty (30) calendar days' written notice shall be given to CalMHSA prior to cancellation of such policy; and, shall waive all rights of subrogation against the additional insureds. The additional insured endorsement issued on the commercial general liability policy shall be a CG 2010 or equivalent.
G. Contractor shall notify CalMHSA of any material change in each policy required under this Section at least thirty (30) calendar days prior to any such change. Contractor shall immediately, and in no instance later than seven (7) calendar days after, notify CalMHSA in the event of the cancellation or failure to renew of any policy required in this Section.
H. As to any policy of insurance required by this Section, Contractor shall disclose any self-insured retention or deductible exceeding $5,000. CalMHSA may require that an endorsement be obtained reducing or eliminating such self-insured retention or deductible as to the CalMHSA

and its officers, agents, board and employees; or may require Contractor to provide a financial guarantee guaranteeing payment of any necessary expenses of investigation, costs of defense, settlement or judgments.

I. Prior to commencing work, and with no additional request from CalMHSA, Contractor shall deliver to CalMHSA certificates of insurance ('COI") and at the beginning of each new year of the Term and any COIs for professional liability coverage for each of the 4 years following the end of the Term per Section C, as well as any required additional insured endorsements demonstrating compliance with these requirements. Upon request by CalMHSA, Contractor shall provide copies of any required insurance policies within ten (10) business days. In the event Contractor fails to secure or maintain any required policy of insurance, CalMHSA may, at its sole discretion, terminate this Agreement, or secure such insurance in the name of and for the account of Contractor, and in such event, Contractor shall reimburse CalMHSA upon demand for the cost thereof. Any failure of CalMHSA to require certificates of insurance and additional insured endorsements shall not operate as a waiver of these requirements.

J. If Contractor does not include all subcontractors as insureds under Contractor's own policies, Contractors shall provide CalMHSA with each subcontractor's evidence of insurance coverage as required of Contractor. Contractor shall be responsible for verifying each subcontractor complies with the required insurance provisions herein and shall require that each subcontractor name CalMHSA and Contractor as additional insureds on the subcontractor's commercial general liability policy. Contractor shall obtain CalMHSA's prior written approval of any subcontractor request for modification of the required insurance.

K. Certificate holder on the policy as "California Mental Health Services Authority (CalMHSA) 1610 Arden Way, Suite 175, Sacramento, CA 95815"

7. INDEPENDENT CONTRACTOR. Contractor is an independent contractor and no employer and employee is created by this Agreement. The contractor and its employees shall not be considered officers, employees or agents of CalMHSA. CalMHSA shall not be liable for any acts or omissions of, nor for any obligations or liabilities incurred by, Contractor, its employees, consultants or subcontractors. Contractor shall have no claim under this Agreement or otherwise, for seniority, vacation time, vacation pay, sick leave, personal time off, overtime, health insurance medical care, hospital care, retirement benefits, social security, disability, Workers' Compensation, or unemployment insurance benefits, civil service protection, or employee benefits of any kind. Contractor assumes full responsibility for its acts and/or omissions as they relate to the Services to be provided under this Agreement. Contractor is solely responsible for payment of all federal, state and local taxes or contributions, including unemployment insurance, social security and income taxes. Contractor agrees to indemnify and hold CalMHSA harmless from any and all liability which CalMHSA may incur because of Contractor's failure to pay such amounts.

8. CONFIDENTIALITY. During performance of this Agreement, information and data of a confidential or proprietary nature may be disclosed to the Contractor. Such information which is disclosed by CalMHSA to Contractor, its employees, or its subcontractors during the Term and which is not available in the public

domain, already known by the Contractor, or independently developed by the Contractor (hereafter referred to as "Confidential Information"), shall be considered by Contractor as confidential in nature. Contractor agrees to accept such data in confidence, to not disclose such data to others, to comply with all applicable state and federal laws, including all laws governing the confidentiality of patient information and health records, and to refrain from using such data for purposes other than those permitted by the Agreement. Contractor shall be governed by all statutory guarantees of client confidentiality in handling any documents related to specific clients. Contractor may engage in activities with CalMHSA and counties, cities, or other regions to share data for the coordination of public presentations and other purposes as deemed appropriate and acceptable by both parties. Contractor shall use Confidential Information only for internal purposes which are directly related to the duties set out in this Agreement. In the absence of any written consent by CalMHSA, Contractor agrees to use all reasonable and practicable efforts to prevent disclosure of Confidential Information to third parties. It is understood that this obligation of confidentiality shall not apply to information that (a) is already in Contractor's possession at the time of disclosure thereof, (b) is or later becomes part of the public domain through no fault of Contractor, (c) is received by Contractor from a third party having no obligations of confidentiality to CalMHSA, (d) is independently developed by Contractor, or (e) is required by law or regulation to be disclosed. Upon expiration or early termination of this Agreement, Contractor shall, at CalMHSA's sole discretion, destroy or otherwise dispose of the confidential information subject to this Section. Contractor must agree to all confidentiality requirements set forth above prior to commencing work under this Agreement.

9. INTELLECTUAL PROPERTY. Contractor hereby assigns ownership of all nonproprietary data, documents, and reports produced under this Agreement ("works") to CalMHSA. Contractor agrees to cause its agents and employees to execute any documents necessary to secure or perfect CalMHSA's legal rights and worldwide ownership in such materials, including documents relating to patent, trademark and copyright applications. Contractor is authorized to maintain a copy of all information necessary to comply with its contractual obligations and applicable professional standards. Notwithstanding the foregoing, Contractor's Intellectual Property ("Contractor IP") that pre-exists this Agreement shall remain the sole and exclusive property of Contractor. Contractor shall not incorporate any Contractor IP into the works prepared pursuant to this Agreement that would limit CalMHSA's use of the works without Contractor's written approval. To the extent that Contractor incorporates any Contractor IP into the Works, Contractor hereby grants to CalMHSA a non-exclusive, non-transferable, perpetual, worldwide, royalty-free license to use and reproduce the Contractor IP to the extent required to utilize the works solely in connection with Contractor's use of the deliverable works. Contractor acknowledges and agrees that, notwithstanding any provision herein to the contrary, CalMHSA's Intellectual Property ("CalMHSA IP") in the information, documents and other materials provided to Contractor shall remain the sole and exclusive property of CalMHSA, and CalMHSA grants to Contractor a non-exclusive, royalty-free, non-transferable license to use and reproduce CalMHSA IP solely for the purposes of performing its obligations under this Agreement. Any information, documents or materials provided by CalMHSA pursuant to this Agreement and all copies thereof (including Confidential Information) shall upon the earlier of CalMHSA's

request or the expiration or termination of this Agreement be returned to CalMHSA, unless retention is permitted or required by the Agreement.

10. TERMINATION. For Convenience: Either party may terminate this Agreement for convenience at any time upon giving the other party thirty (30) calendar days' written notice. If such notice is given by CalMHSA, upon receipt, Contractor shall stop all work in a timely manner and use its reasonable efforts to limit any outstanding financial commitments under this Agreement. Contractor shall reimburse CalMHSA for any advance funds received and shall only retain the appropriate amount for any of the Services provided up to the date of notice, including non-cancellable obligations. In the event CalMHSA terminates Contractor's work for convenience, Contractor shall be entitled to payment for any of the Services provided prior to the effective date of said termination, subject to the terms of the Agreement. **For Cause:** Failure of either party to comply with any material provision of this Agreement shall constitute a material breach. In the event of such a breach the non-breaching party will notify the breaching party of such determination and afford the breaching party a reasonable time period within which to cure the breach; the breaching party shall provide a plan for correction within fifteen (15) business days of notification of breach; the non-breaching party shall provide an approval or rejection of such plan within ten (10) business days of receipt of plan; and the non-breaching party may withhold payment during breach. Should the parties not reach consensus on the correction plan or should the breaching party not correct the deficiencies within the period agreed to by the parties, the non-breaching party may terminate this Agreement immediately by written notice of termination. If Contractor fails to perform as required under the Agreement, CalMHSA may recover or deduct from amounts otherwise owing under the Agreement any costs it sustains resulting from Contractor's breach. Upon receipt of notice of termination pursuant to this Section, Contractor shall stop work as of the date specified, and transfer to CalMHSA any materials that would have been required to be furnished to CalMHSA. In addition, the non-breaching party may avail itself of any other remedies available at law or under this Agreement.

11. INDEMNIFICATION. Contractor shall indemnify, hold harmless and defend CalMHSA, its officers, directors, employees, agents, members and consultants from and against any and all claims, costs, losses, fees, penalties, fines, injury, damage(s) and liabilities arising from the Services or work provided or to be provided under the Agreement or due to Contractor's failure to comply with the term of the Agreement.

12. AUDITS; ACCESS TO RECORDS. Contractor agrees that CalMHSA, or its designated representative shall have the right to review and to copy any records and supporting documentation pertaining to the performance of this Agreement. Contractor agrees to maintain such records for possible audit for a minimum of three (3) years after final payment unless a longer period of records retention is stipulated. Contractor agrees to allow the auditor(s) access to such records during normal business hours and to allow interviews of any employees who might reasonably have information related to such records. Further, in the event the value of this Agreement exceeds $10,000, Contractor understands that the State of California may audit records and interview staff regarding any contract or subcontract related to performance of this Agreement. (Gov. Code §8546.7, Pub. Contract Code §10115 et seq., CCR Title 2,

Section 1896). If such records are not kept and maintained by Contractor within the State of California, Contractor shall, upon request of CalMHSA, make such records available to CalMHSA for inspection at a location within the state or Contractor shall pay to CalMHSA the reasonable, and necessary costs incurred by CalMHSA in inspecting Contractor's records, including, but not limited to, travel, lodging and subsistence costs. Contractor shall provide such assistance as may be reasonably required in the course of such inspection. Upon request by CalMHSA, Contractor shall provide CalMHSA a copy of Contractor's most recent compiled, reviewed or audited financial reports. CalMHSA may request updated reports during the term of the contract.

13. PUBLIC RECORDS. All correspondence, documents, records, or other written materials submitted to CalMHSA become the exclusive property of CalMHSA, and are therefore potentially subject to disclosure under the California Public Records Act ("CPRA"; see Govt. Code Section 6250 et seq.).

14. AMENDMENT. No amendment or variation of the terms of this Agreement (including but not limited to the Scope of Work) shall be valid unless made in writing signed by the parties. No oral understanding or agreement not incorporated in this Agreement is binding on any of the parties.

15. QUALIFICATION TO DO BUSINESS IN CALIFORNIA. Contractor hereby certifies that its directors, officers, partners, agents, employees, and subcontractors have obtained and maintain all licenses, permits, certifications, and other documents necessary for Contractor's performance of this Agreement. Contractor shall immediately notify CalMHSA of any suspension, termination, lapses, non-renewals, or restrictions of licenses, permits, certificates, or other documents that relate to Contractor's performance of this Contract and qualification to do business in the State of California.

16. DISPUTES/ALTERNATIVE DISPUTE RESOLUTION. During any dispute, Contractor shall continue with the responsibilities under this Agreement, unless directed otherwise by CalMHSA in writing. Disputes do not include the Contractor's failure to perform any requirements under this Agreement, and this Agreement may be terminated by CalMHSA with or without cause without following the dispute process. The parties agree that any dispute or claim arising out of or relating to the Agreement or the services provided hereunder shall first be submitted to non-binding mediation as a prerequisite to litigation. Mediation may take place at a location designated by the parties. If, after good faith efforts, the parties are unable to resolve their dispute through mediation within ninety (90) calendar days after the issuance by one of the parties of a request for mediation, then the parties are free to pursue all other legal and equitable remedies available to them. Nothing herein shall preclude Contractor from filing a timely formal claim in accordance with applicable California law provided, however, that Contractor shall, if permitted, seek a stay of said claim during the pendency of any mediation. Either party may seek to enforce any written agreement reached by the parties during mediation in any court of competent jurisdiction.

17. FINAL SETTLEMENT. Contractor agrees to maintain and retain all appropriate records and allow access to those records as provided in this Agreement. Contractor agrees to furnish duly authorized representatives from CalMHSA access to records and to disclose to CalMHSA representatives all financial Standard Services Agreement - Exhibit

records necessary to review the Services and to evaluate the cost, quality, appropriateness and timeliness of same. If the appropriate court, federal or state agency, or CalMHSA, determines that all, or any part of, the payments made by CalMHSA to Contractor pursuant hereto are or were not payable in accordance with this Agreement, or any other applicable provision of law, ordinance, code, regulation, contract, or applicable agreement; or that the Contractor, its officers, agents, employees or subcontractor committed fraud or abuse in connection with work arising out of the performance of this Agreement, said payments or related amounts shall be repaid on demand by Contractor to CalMHSA. Prior to receiving final payment hereunder, Contractor shall submit a signed, written release discharging CalMHSA, its officers and staff, from all liabilities, obligations, and claims arising out of or under the Agreement, except for any claims specifically described in detail in such release. At the conclusion of the Services to be provided hereunder this Agreement, and as part of the content to be delivered to CalMHSA and its agents hereunder, Contractor shall execute any documents necessary to effectuate any transfer of rights described in this Agreement. Contractor shall also arrange for execution of any necessary documents by those subcontractors, if any, involved in any development of work as to which CalMHSA is obtaining rights pursuant to this Agreement.

18. INSPECTION OF DOCUMENTS AND MATERIALS. Contractor shall maintain and make available to CalMHSA for its inspection and use during the term of this Agreement, all documents and materials required to be provided to CalMHSA under this Agreement. Contractor's obligations hereunder shall continue for three years following termination or expiration of this Agreement or the completion of all work hereunder (as evidenced in writing by CalMHSA), and Contractor shall in no event dispose of, destroy, alter or mutilate said documents and materials, for three years following CalMHSA's last payment to Contractor under this Agreement. It is the responsibility of Contractor to ensure all documents and materials comply with applicable industry regulations and standards.

19. CONFLICT OF INTEREST PROHIBITION. Contractor represents and warrants that Contractor has no business, professional, personal, or other interest that would conflict in any manner with the performance of its obligations under this Agreement. If any such actual or potential conflict of interest arises, Contractor shall immediately inform CalMHSA in writing of such conflict and If, in the reasonable judgment of CalMHSA, such conflict poses a material conflict to and with the performance of Contractor's obligations under this Agreement, then CalMHSA may terminate the Agreement immediately upon written notice to Contractor with such termination effective upon notice receipt.

20. USE OF PUBLIC FUNDS. Contractor, including its officers and members, shall not use funds received from CalMHSA pursuant to this Agreement to support or pay for costs or expenses related to campaigning or other partisan activities to advocate for either the election or defeat of any candidate for elective office, or for or against the passage of any proposition or ballot measure; or lobbying for either the passage or defeat of any legislation. This provision is not intended and shall not be construed to limit any expression of a view, opinion, or position of any member of Contractor as an individual or private citizen, as long as

public funds are not used; nor does this provision limit Contractor from merely reporting the results of a poll or survey of its membership.

21. **DISCLAIMER OF RESPONSIBILITY FOR CONTENT OF CONTRACTOR'S PUBLICATIONS.** CalMHSA will not be responsible for the content of Contractor's publications, whether electronic, broadcast, printed, or otherwise. If CalMHSA is identified as a sponsor of, or otherwise identified in, Contractor's website, blog, social media page, or other site, and if Contractor allows members of the public to contribute to its website, blog, social media page, or other site, Contractor shall display a disclaimer substantially similar to the following:

> All information, data, text, software, music, sound, photographs, video, messages, blog posts, user comments and other materials, whether publicly posted or privately transmitted, are the sole responsibility of the individual source of said content. Individuals using this site are entirely responsible for the content they upload, post, e-mail, transmit, or otherwise make available here. [insert Contractor name] and CalMHSA are in no way responsible for the content posted here, and therefore cannot guarantee its accuracy, integrity, or quality. By using this site, you may be exposed to content that is offensive or objectionable. Under no circumstances are we liable for content that includes errors or omissions, or for loss or damage of any kind incurred as a result of using this site's content.

22. **CO-MARKETING/USE OF BRANDING**. The parties may agree to co-operate together and co-market successful work and Services completed as part of this Agreement or any part thereof related to a Program but are not required to do so. Each party must consent to any proposed marketing or co-marketing related to the Services provided under the Agreement, including the scope, channel(s), content and limitations of same. Neither party may use the other party's name, copyrights, trademarks, branding, IP, content, social media channels, or content protections without the written consent of the other party nor disparage the other party and if the parties agree to allow marketing jointly or otherwise, the posting party must follow the branding guidelines of the non-posting party. The parties may also agree to collaborate on publicity content upon the written consent of both parties regarding the concept, form, channel, content and related items.

23. FORCE MAJEURE. The following shall be considered force majeure events: revolutions, insurrections, riots, wars, acts of enemies, pandemics (except for Covid-19), government-declared emergencies, strikes, floods, fires, acts of god, or any cause, whether of the class of causes enumerated above or not, that is outside the control of the party whose performance is or will be impaired and which such party is unable to prevent by the exercise of reasonable diligence. Upon occurrence of a force majeure event, the non-performing party shall promptly notify the other party that a force majeure event has occurred and explain its anticipated effect on performance, including its expected duration. The non-performing party shall furnish the other party with periodic reports regarding the progress of the force majeure event. The

non-performing party shall use reasonable diligence to minimize damages and to resume performance. If the parties agree that because of the force majeure event the purposes of the Agreement will be substantially frustrated, the Agreement will be deemed to have been terminated as of the time of such agreement, and the obligations of the parties will be those set forth in the Termination section regarding contracts terminated for convenience.

24. **PUBLIC HEARINGS.** If public hearings on a subject matter dealt with in the Agreement are held within one year from the Agreement expiration date to the extent that it can do so, Contractor shall make available to testify the personnel assigned to the Agreement at the actual rates of compensation of such personnel. CalMHSA shall reimburse Contractor for actual travel and compensation costs of said personnel for such testimony as may be requested by CalMHSA. Compensation and travel rates may not exceed those normally permissible by Contractor under its own policies or regulations.

25. NON-DISCRIMINATION. During the performance of this Agreement, Contractor and its subcontractors shall not deny the 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, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status. Contractor shall ensure that the evaluation and treatment of employees and applicants for employment are free of such discrimination. Contractor and subcontractors shall comply with the provisions of the Fair Employment and Housing Act (Gov. Code §12900 et seq.), the regulations promulgated thereunder (Cal. Code Regs., tit. 2, §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 CalMHSA to implement such articles. Contractor shall permit access by representatives of the Department of Fair Employment and Housing and CalMHSA upon reasonable notice at any time during the 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 CalMHSA shall require to ascertain compliance with this clause. Contractor and its subcontractors shall give written notice of their obligations under this clause to labor organizations with which they have a collective bargaining or other agreement. (See Cal. Code Regs., tit. 2, §11105.) Contractor shall include the nondiscrimination and compliance provisions of this clause in all subcontracts to perform work under the Agreement.

26. TIME OF ESSENCE. Time is of the essence in respect to all provisions of this Agreement that specify a time for performance; provided, however, that the foregoing shall not be construed to limit or deprive a party of the benefits of any grace or use period allowed in this Agreement.

27. GOVERNING LAW. This Agreement shall be governed by the laws of the State of California without regard to its choice of law provisions.

28. SUBSTITUTION/NON-DELEGATION. Contractor's key personnel may not be substituted without notice to and non-objection by CalMHSA. Contractor shall not subcontract, assign or delegate any portion of this Agreement's duties or obligations hereunder without CalMHSA's prior written approval.

29. WAIVER. No waiver of a breach, failure of any condition, or any right or remedy contained in or granted by this Agreement shall be effective unless it is in writing and signed by the party waiving the breach, failure, right or remedy. No waiver of any breach, failure, right or remedy shall be deemed a waiver of any other breach, failure, right or remedy, whether or not similar, nor shall any waiver constitute a continuing waiver unless the writing so specifies.

30. ENTIRE AGREEMENT. This Agreement, including all attachments, exhibits, and any other documents specifically incorporated into this Agreement, shall constitute the entire agreement between CalMHSA and Contractor relating to its subject matter. This Agreement supersedes and merges all previous understandings, and all other agreements, written or oral, between the parties.

31. SURVIVAL. The obligations of this Agreement, which by their nature would continue beyond the termination on expiration of the Agreement, including without limitation, Indemnification, Final Settlement, Intellectual Property, Confidentiality, and Audits/Access to Records, shall survive termination or expiration.

32. SEVERABILITY. If an administrative tribunal or court of competent jurisdiction holds any provision of this Agreement, or the application of any provision or part, to be illegal, unenforceable, or invalid in whole or in part, the validity and enforceability of the remaining provisions, or portions or applications of them, shall remain valid and enforceable to the fullest extent permitted by law.

33. NOTICE. All notices, requests, demands, or communications under this Agreement shall be in writing unless otherwise noted in this Agreement. Notices shall be given as follows: Personal delivery: When personally delivered to the recipient, notice is effective on delivery; First Class Mail: When mailed first class to the last address of the recipient known to the party giving notice, notice is effective three (3) mail delivery days after deposit in a USPS office or mailbox.; Certified Mail: When mailed certified mail, return receipt requested, notice is effective on receipt, if delivery is confirmed by a return receipt; Overnight Delivery: When delivered by overnight delivery with charges prepaid or charged to the sender's account, notice is effective on delivery, if delivery is confirmed by the delivery service; Email: When delivered via email, notice is effective upon (i) a "received" or "read" receipt when the sender has no reason to believe the party being emailed will not receive the message, or (ii) upon acknowledgement of receipt by the recipient. Any correctly addressed notice that is refused, unclaimed, or undeliverable because of an act or omission of the party to be notified shall be deemed effective as of the first date that said notice was refused, unclaimed, or deemed undeliverable by the delivery service.

34. AUTHORITY TO SIGN. By signing this agreement, signatory warrants and represents that he/she executed this Agreement in his/her authorized capacity and that by his/her signature on this Agreement, he/she or the entity upon behalf of which he/she acted, executed this Agreement.

END OF SECTION– EXHIBITS FOLLOW

Exhibit A – Funding Allocation Form

[Insert budget table – deliverable based]

NOTE: The above funding allocation is based on deliverables completed and is subject to change due to assessments made over time. Supporting documentation for each completed deliverable and approval email from _____ County must be attached to each invoice.

Upon submission of each deliverable to CalMHSA by the Contractor, CalMHSA will review for approval and/or request changes within three (3) business days of submission. Following each subsequent submission of edited deliverables, CalMHSA will have an additional three (3) business days to review for approval. Deliverables will be deemed completed and accepted upon CalMHSA's written (email acceptable) final approval, at which time the Contractor may submit an invoice.

Exhibit B – Privacy and Data Security Policy

PRIVACY AND SECURITY REQUIREMENTS

A. **Purpose of Exhibit.** This Exhibit sets forth the privacy and security requirements that apply to all Personally Identifiable Information (PII) that Contractor obtains, maintains, transmits, uses or discloses from or to CalMHSA or County Members pursuant to this Agreement. The parties agree to all terms and conditions of this Exhibit to ensure the integrity, security, and confidentiality of the information exchanged pursuant to this Agreement and to allow disclosure and use of such information only as permitted by law and only to the extent necessary to perform functions and activities pursuant to this Agreement. This Exhibit establishes requirements in accordance with applicable federal and state privacy and security laws including, but not limited to, the Information Practices Act (California Civil Code section 1798 et seq.), and where applicable, the Health Insurance Portability and Accountability Act (42 U.S.C. section 1320d-d8), and the Health Information Technology for Economic and Clinical Health Act and their implementing regulations at 45 C.F.R. Parts 160 and 164 (collectively, "HIPAA").

B. **Definitions.** The following definitions shall apply to this Exhibit:

1. **Breach**: Shall mean either: i) the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical, or electronic; or ii) a reasonable belief that unauthorized acquisition of PII that compromises the security, confidentiality or integrity of the PII has occurred

2. **Disclosure**: The release, transfer, provision of access to, or divulging in any other manner of PII outside the entity holding the information.

3. **Personal Information or** PI: Information that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual. (California Civil Code section 1798.3)

4. **Personally Identifiable Information or PII**: Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name,

etc. (OMB M-07-16.) PII includes Federal Tax Information (FTI), Personal Information (PI) and Protected Health Information (PHI).

5. **Protected Health Information or PHI:** Individually Identifiable Health Information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as defined in 45 C.F.R. section 160.103.

6. **Security Incident:** The act of violating an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction. Adverse events such as floods, fires, electrical outages, and excessive heat are not considered incidents. (Computer Matching Agreement, Agreement No. 2013-11, p.5.)

C. **Applicable Laws.** Contractor shall comply with all federal and state privacy and security laws, including but not limited to the Health Insurance Portability and Accountability Act (42 U.S.C. section 1320d-d8), the Health Information Technology for Economic and Clinical Health Act and their implementing regulations at 45 C.F.R. Parts 160 and 164 (collectively, "HIPAA"), and the Information Practices Act of 1977, California Civil Code section 1798 et seq. To the extent a conflict arises between any laws or other requirements, Contractor agrees to comply with the applicable requirements imposing the more stringent privacy and security standards.

D. **Security Controls and Safeguards**

1. **Safeguards**: At a minimum, contractor shall establish and implement operational, technical, administrative and physical safeguards consistent with any applicable laws to ensure:

   a. The confidentiality, integrity, and availability of personally identifiable information created, collected, used, and/or disclosed by CalMHSA or its County Members;
   b. Personally identifiable information is only used by or disclosed to those authorized to receive or view it;
   c. Personally identifiable information is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information;
   d. Personally identifiable information is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law; and
   e. Personally identifiable information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules.

2. **Encryption:** Contractor shall encrypt all PII that is in motion or at rest, including but not limited to data on portable media devices, using commercially reasonable means, consistent with

applicable Federal and State laws, regulations and agency guidance, including but not limited to the U.S. Department of Health and Human Services guidance specifying the technologies and methodologies that render PII unusable, unreadable, or indecipherable to unauthorized individuals for purposes of the breach notification requirements or issued by the National Institute for Standards and Technology ("NIST") concerning the protection of identifiable data such as PII. Data centers shall be encrypted or shall otherwise comply with industry data security best practices.

3. **Hardware:** Contractor shall ensure that any and all hardware, including but not limited to personal computers, laptops, jump-drives, smart phones or other devices upon which PII is stored, is secured, password-protected and only accessible by Contractor or Contractor's agents, employees or sub-contractors in accordance with the terms of this Exhibit. Contractor shall at all times remove and permanently delete any and all PII before any such hardware is transferred or sold to a third-party or is otherwise subject to any change in ownership or control.

4. **Log-In Credentials**: Contractor shall at all times ensure that each individual user of any CalMHSA or County Member computer system through which PII is accessed maintains his or her own unique user-id and password. Contractor shall strictly refrain from sharing individual log-in credentials and shall at all times assume responsibility for ensuring that the log-in credentials of any former employees, sub-contractors, agents or other representatives who are no longer subject to this Agreement are de-activated or otherwise changed to prevent unauthorized access by any such individuals.

5. Contractor shall update these safeguards as appropriate and as requested by CalMHSA.

E. **Policies and Procedures:**

1. Contractor shall implement and maintain written policies and procedures to ensure the privacy and security of PII stored, maintained, or accessed in compliance with this Agreement and any applicable laws. Such policies shall address

   a. Implementation of consumer rights as required by this Exhibit;
   b. Reasonable safeguards as required by this Exhibit;
   c. Monitoring, periodically assessing, and updating security controls and related system risks to ensure the continued effectiveness of those controls; and
   d. Training employees, contractors, and subcontractors.

2. Upon request, Contractor shall provide CalMHSA with a written policies and procedures adopted by Contractor to meet its obligations under this Section.

F. **Subcontractors**. Contractor shall be bound by and be responsible for the acts and omissions of its subcontractors, agents or vendors in the exchange of data with CalMHSA. Contractor shall take reasonable steps to ensure compliance with the Agreement by its subcontractors, agents and

vendors. Contractor agrees to enter into written contracts with its agents and contractors (collectively, "subcontractors") that obligate Contractor's subcontractors to abide by the same privacy and security standards and obligations that Contractor has agreed to in this Agreement. Contractor represents and agrees that it shall only request that CalMHSA transmit data to subcontractors with whom it has such agreements and only to the extent such information is necessary to carry out the purposes authorized by this Agreement. Upon request, Contractor shall provide CalMHSA with a copy of any written agreement or contract entered into by Contractor and its subcontractors to meet the obligations of Contractor under this Exhibit.

G. Breaches & Security Incidents

1. Contractor shall immediately report to CalMHSA any actual or suspected Breaches or Security Incidents involving PII created or received under this Agreement. Contractor's report shall contain the following information to the extent applicable and known at that time:

    a. A brief description of what happened including the date of the incident and the date of the discovery of the incident;
    b. The names or identification numbers of the individuals whose PII has been, or is reasonably believed to have been accessed, acquired, used or disclosed;
    c. A description of the types of PII that were involved in the incident, as applicable;
    d. Information regarding any information system intrusion and any systems potentially compromised;
    e. A brief description of Contractor's investigation and mitigation plan; and
    f. Any other information necessary for CalMHSA to investigate and include in notifications to the individual(s) or relevant regulatory authorities under applicable privacy and security requirements.

2. Upon completion of the initial report, Contractor shall immediately commence an investigation in accordance with applicable law to determine the scope of the incident; mitigate harm that may result from the incident; and restore the security of the system to prevent any further harm or incidents.

3. Contractor shall cooperate with CalMHSA in investigating the actual or suspected incident and in meeting CalMHSA's obligations, if any, under applicable laws.

4. Contractor shall mitigate to the extent practicable any harmful effect of any Incident that is known or reasonably discoverable to Contractor.

5. After conducting its investigation, and within fifteen (15) calendar days, unless an extension is granted by CalMHSA, Contractor shall file a complete report with the information listed above in subsection (1), if available. Contractor shall make all reasonable efforts to obtain all relevant information and shall provide an explanation if any information cannot be obtained. The complete report shall include a corrective action plan that describes the steps to be taken to prevent any future re-occurrence of the incident.

6. Contractor shall cooperate with CalMHSA in developing content for any public statements and shall not give any public statements without the express written permission of CalMHSA.

7. If a Breach requires notifications and reporting under applicable laws and the cause of the Breach is attributable to Contractor, its agents or subcontractors, Contractor shall Be fully responsible for providing breach notifications and reporting as required under applicable laws; pay any costs of such Breach notifications as well as any costs or damages associated with the incident; and should CalMHSA in its sole discretion determine that credit monitoring is an appropriate remedy, arrange for and bear the reasonable, out-of-pocket cost of providing to each such affected individual one (1) year of credit monitoring services from a nationally recognized supplier of such services.

8. If Contractor determines that an impermissible acquisition, use, or disclosure of PII does not require breach notifications or reporting, it shall document its assessment and provide such documentation to CalMHSA within one week of its completion. Notwithstanding the foregoing, CalMHSA reserves the right to reject Contractor's assessment and direct Contractor to treat the incident as a Breach.

H. **Right to Inspect.** CalMHSA may inspect the facilities, systems, books, and records of Contractor to monitor compliance with this Exhibit at any time. Contractor shall promptly remedy any violation reported to it by CalMHSA and shall certify the same to CalMHSA in writing. The fact that CalMHSA inspects, fails to inspect, fails to detect violations of this Exhibit or detects but fails to notify Contractor of the violation or require remediation is not a waiver of CalMHSA's rights under the Agreement and this Exhibit.

I. **Indemnification.** Contractor shall indemnify, hold harmless, and defend CalMHSA from and against any and all costs (including mailing, labor, administrative costs, vendor charges, and any other costs CalMHSA determines to be reasonable), losses, penalties, fines, and liabilities arising from or due to Contractor's failure to comply with the requirements of this Exhibit, including a breach or other non-permitted use or disclosure of PII by Contractor or its subcontractors or agents. CalMHSA shall give notice of any claims to Contractor after discovery thereof. If Contractor should publish or disclose PII to others, CalMHSA shall be entitled to injunctive relief or any other remedies to which it is entitled under law or equity, without posting a bond.

J. **Termination of Agreement.** If Contractor breaches its obligations under this Exhibit as determined by CalMHSA, CalMHSA may, at its option: Require Contractor to submit to a plan of monitoring and reporting that CalMHSA may deem necessary to maintain compliance with this Agreement; provide Contractor with an opportunity to cure the breach; or after giving Contractor an opportunity to cure the breach, or upon breach of a material term of this Exhibit, terminate this Agreement for cause. A failure of CalMHSA to exercise any of these options shall not constitute a waiver of its rights hereunder. Upon expiry or termination of the Agreement, at CalMHSA's direction, Contractor shall either return all PII to CalMHSA, or shall destroy all PII in a manner consistent with applicable State and Federal laws, regulations, and agency guidance on

the destruction of PII. If return or destruction of PII is not feasible, Contractor shall explain in writing to CalMHSA why return or destruction is not feasible. The obligations of Contractor under the Agreement to protect PII and to limit its use or disclosure shall continue and shall survive until all PII is either returned to CalMHSA or destroyed.

SUB-BUSINESS ASSOCIATE AGREEMENT

UNDER THE HEALTH INSURANCE PORTABILITY

AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

This Sub-Business Associate Agreement (this "Sub-Business Associate Agreement"), is made by and among the California Mental Health Services Authority ("CalMHSA"), and _____ ("Contractor").

CalMHSA and Contractor have entered into an agreement (the "Contract") pursuant to which Contractor performs certain services for CalMHSA for the benefit of its "Participants".

Participants include Counties, Cities and other local government authorities (e.g., Joint Powers Authorities), and are Covered Entities 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"). In connection with Contractor providing services to CalMHSA pursuant to the Contract, Contractor may, on behalf of CalMHSA, create, receive, maintain, or transmit certain Protected Health Information, as defined by the HIPAA Rules, on behalf of one or more Covered Entity Participants.

As such, CalMHSA is a Business Associate and Contractor is a Sub-Business Associate of CalMHSA, and is therefore subject to those provisions of the HIPAA Rules that are applicable to Business Associates.

The HIPAA Rules require a written agreement between CalMHSA 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 CalMHSA 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 Sub-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" and/or a "sub-business associate" also is a subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of another business associate.

1.3 "Covered Entity" has the same meaning as the term "covered entity" at 45 CFR § 160.103, and in reference to the party to this Sub-Business Associate Agreement, "Covered Entity" shall mean one or more Covered Entity Participants whose Protected Health Information is being created, received, maintained, accessed or transmitted by Contractor.

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

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

1.6 "Designated Record Set" has the same meaning as the term "designated record set" at 45 C.F.R. § 164.501.

1.7 "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 a Business Associate's internal operations or to other than its workforce. (See 45 C.F.R. § 160.103.)

1.8 "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.)

1.9 "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: (i) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; (ii) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

1.10 "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 Contractor from or on behalf of CalMHSA and Covered Entity Participants. For the convenience of the Parties, Electronic Protected Health Information means Protected Health Information that is: (i) transmitted by electronic media; and/or (ii) maintained in electronic media.

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

1.12 "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).

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

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

1.15 "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 Contractor from or on behalf of CalMHSA and Covered Entity Participants. 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 Contractor from or on behalf of CalMHSA or a Covered Entity Participant, and includes Protected Health Information that is made accessible to Contractor by CalMHSA and a Covered Entity Participant. "Protected Health Information" includes Electronic Protected Health Information.

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

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

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

1.19 "Services" means, unless otherwise specified, those functions, activities, or services in the Contract, together with any otherwise applicable underlying agreement, contract,

master agreement, work order, or purchase order or other service arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

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

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

1.22 "Use" or "Uses" means, with respect to Protected Health Information, the sharing, employment, application, utilization, examination or analysis of such Information within Contractor's internal operations. (See 45 C.F.R § 164.103.)

1.23 Terms used, but not otherwise defined in the Contract or this Sub-Business Associate Agreement, have the same meaning as those terms in the HIPAA Rules. If there is a conflict between the definitions in this Sub-Business Associate Agreement and the definitions in the HIPAA Rules, the definitions in the HIPAA Rules shall control.

2. Permitted and Required Uses and Disclosures of Protected Health Information

2.1 Contractor 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 Sub-Business Associate Agreement.

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

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

2.4 Contractor shall make Uses and Disclosures and requests for Protected Health Information consistent with the applicable Covered Entity's Minimum Necessary policies and procedures.

2.5 Contractor 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 Contractor 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.

2.7 Contractor may provide Data Aggregation services if such Data Aggregation services are necessary in order to provide Services.

3. Prohibited Uses and Disclosures of Protected Health Information

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

3.2 Contractor shall not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity or CalMHSA, except for the specific Uses and Disclosures set forth in Sections 2, 7, and 8.

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

4.2 Contractor 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 Sub-Business Associate Agreement.

5. Reporting Non-Permitted Uses or Disclosures, Security Incidents, and Breaches of Unsecured Protected Health Information

5.1 Contractor shall report to CalMHSA and all affected Covered Entity Participants any Use or Disclosure of Protected Health Information not permitted by this Sub-Business Associate Agreement, any successful Security Incident, and/ or any Breach of Unsecured Protected Health Information as further described in Sections 5.1(a), 5.1(b), and 5.1(c).

(a) Contractor shall report to CalMHSA and all affected Covered Entity Participants any Use or Disclosure of Protected Health Information by Contractor, its employees, representatives, agents or Subcontractors not provided for by the Contract of which Contractor becomes aware.

(b) Contractor shall report to CalMHSA and all affected Covered Entity Participants any successful Security Incident of which Contractor becomes aware.

(c) Contractor shall report to CalMHSA and all affected Covered Entity Participants any Breach by Contractor, its employees, representatives, agents, workforce members, or Subcontractors of Unsecured Protected Health Information that is known to Contractor or, by exercising reasonable diligence, would have been known to Contractor. Contractor 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 Contractor, 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, Contractor shall provide, to the extent available, all information required by, and within the times frames specified in, Sections 5.2(a) and 5.2(b)(i).

(a) Contractor shall make an immediate telephonic report upon discovery of the non-permitted Use or Disclosure of Protected Health Information, successful Security Incident, or Breach of Unsecured Protected Health Information to the CalMHSA Privacy Officer that minimally includes:

(i) A brief description of what happened, including the date and time 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;

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

(iii) 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);

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

(b) Contractor shall make a written report without unreasonable delay and in no event later than three (3) business days from the date of discovery by Contractor of the non-permitted Use or Disclosure of Protected Health Information, successful Security Incident, or Breach of Unsecured Protected Health Information to the CalMHSA Privacy Officer t, that includes, to the extent possible:

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

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

(iii) 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);

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

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

(vi) Any steps Contractor 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;

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

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

(c) If Contractor is not able to provide the information specified in this Section 5.2 at the time of the required report, Contractor shall provide such information promptly thereafter as such information becomes available.

5.3 Contractor may delay the notification required by this Section 5, if a Law Enforcement Official states to Contractor that notification would impede a criminal investigation or cause damage to national security.

(a) If the Law Enforcement Official's statement is in writing and specifies the time for which a delay is required, Contractor shall delay it's reporting and/or notification obligation(s) for the time period specified by the official.

(b) If the statement is made orally, Contractor 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(a) 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, Contractor shall ensure that any Subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of Contractor 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 Contractor with respect to such information.

6.2 Contractor 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 Contractor.

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

6.5 Without limiting the requirements of Section 5, the agreement required by Section 6.1 (Subcontractor Contractor Agreement) shall require Subcontractor to contemporaneously notify CalMHSA in the event of a Breach of Unsecured Protected Health Information.

6.6 Without limiting the requirements of Section 19, the agreement required by Section 6.1 shall include a provision requiring Subcontractor to destroy, or in the alternative to return to Contractor, any Protected Health Information created, received, maintained, or transmitted by Subcontractor on behalf of Contractor so as to enable Contractor to comply with the provisions of Section 19.

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

6.8 Sections 6.5 and 6.6 are not intended by the Parties to limit in any way the scope of Contractor'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 CalMHSA determines that Protected Health Information is maintained by Contractor or its agents or Subcontractors in a Designated Record Set, Contractor shall, within two (2) business days after receipt of a request from CalMHSA, make the Protected Health Information specified by CalMHSA available to the Individual(s) identified by CalMHSA as being entitled to access and shall provide such Individuals(s) or other person(s) designated by CalMHSA with a copy the specified Protected Health Information, in order for CalMHSA to meet the requirements of 45 C.F.R. § 164.524.

7.2 If any Individual requests access to Protected Health Information directly from Contractor or its agents or Subcontractors, Contractor shall notify CalMHSA in writing within two (2)

days of the receipt of the request. Whether access shall be provided or denied shall be determined by CalMHSA.

7.3 To the extent that Contractor 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, Contractor 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 CalMHSA and the Individual.

8. Amendment of Protected Health Information

8.1 To the extent CalMHSA determines that any Protected Health Information is maintained by Contractor or its agents or Subcontractors in a Designated Record Set, Contractor shall, within ten (10) business days after receipt of a written request from CalMHSA, make any amendments to such Protected Health Information that are requested by CalMHSA, in order for CalMHSA 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 Contractor or its agents or Subcontractors, Contractor shall notify CalMHSA in writing within five (5) days of the receipt of the request. Whether an amendment shall be granted or denied shall be determined by CalMHSA.

9. Accounting of Disclosures of Protected Health Information

9.1 Contractor shall maintain an accounting of each Disclosure of Protected Health Information made by Contractor or its employees, agents, representatives or Subcontractors, as is determined by CalMHSA to be necessary in order to permit CalMHSA 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.

(a) Any accounting of disclosures provided by Contractor under Section 9.1 shall include:

(i) The date of the Disclosure;

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

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

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

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

9.2 Contractor shall provide to CalMHSA, within ten (10) business days after receipt of a written request from CalMHSA, information collected in accordance with Section 9.1 to permit CalMHSA 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 Contractor or its agents or Subcontractors, Contractor shall notify CalMHSA in writing within five (5) days of the receipt of the request, and shall provide the requested accounting of disclosures to the Individual(s) within 30 days. The information provided in the accounting shall be in accordance with 45 C.F.R. § 164.528.

10. Compliance with Applicable HIPAA Rules

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

10.2 Contractor shall comply with all HIPAA Rules applicable to Contractor in the performance of Services.

11. Availability of Records

11.1 Contractor 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 Contractor on behalf of CalMHSA available to the Secretary for purposes of determining CalMHSA's compliance with the Privacy and Security Regulations.

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

12. Mitigation of Harmful Effects

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

13. Breach Notification to Individuals

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

(a) Contractor shall notify, subject to the review and approval of CalMHSA and each applicable Covered Entity Participant, 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.

(b) The notification provided by Contractor shall be written in plain language, shall be subject to review and approval by CalMHSA and each applicable Covered Entity Participant, and shall include, to the extent possible:

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

(ii) 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);

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

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

(v) 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 The Covered Entity Participant, 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.

13.3 Contractor shall reimburse CalMHSA and each affected Covered Entity Participant any and all costs incurred by CalMHSA, 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 Contractor's Breach of Unsecured Protected Health Information; CalMHSA shall not be responsible for any costs incurred by Contractor in providing the notification required by 13.1 or in establishing the contact procedures required by Section 13.1.

14. DHCS Requirements.

14.1 Contractor and CalMHSA shall comply with the DHCS Requirements provided on Exhibit A-1 and Exhibit A-2 to this Sub-Business Associate Agreement with regard to DHCS PSCI and PII received from CalMHSA. To the extent that any provisions of the DHCS Requirements in Exhibit A-1 or Exhibit A-2 conflict with other provisions of this Sub-

Business Associate Agreement, the more restrictive requirement shall apply with regard to DHCS PSCI or PII received from CalMHSA.

15. Indemnification

15.1 Contractor shall indemnify, defend, and hold harmless CalMHSA and each affected Covered Entity Participant 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 Contractor's acts and/or omissions arising from and/or relating to this Sub-Business Associate Agreement, including, but not limited to, compliance and/or enforcement actions and/or activities, whether formal or informal, by the Secretary or by the Attorney General of the State of California.

15.2 Section 15.1 is not intended by the Parties to limit in any way the scope of Contractor'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, which gives rise to Contractor's status as a Contractor.

16. Obligations of CalMHSA

16.1 CalMHSA shall notify Contractor of any current or future restrictions or limitations on the Use or Disclosure of Protected Health Information of which CalMHSA is aware that would affect Contractor's performance of the Services, and Contractor shall thereafter restrict or limit its own Uses and Disclosures accordingly.

16.2 CalMHSA shall not request Contractor 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 if done by CalMHSA or its Covered Entity Participants, except to the extent that Contractor may Use or Disclose Protected Health Information as provided in Sections 19 and 20 herein.

17. Term

17.1 Unless sooner terminated as set forth in Section 18, the term of this Sub-Business Associate Agreement shall be the same as the term of the applicable underlying agreement, contract, master agreement, work order, purchase order, or other services arrangement, with or without payment, which gives rise to Contractor's status as a Contractor.

17.2 Notwithstanding Section 18, Contractor's obligations under Sections 19 to 20 shall survive the termination or expiration of this Sub-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, 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 Sub-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 Sub-Business Associate Agreement.

18.2 In addition to and notwithstanding the termination provisions set forth in the applicable underlying agreement, contract, master agreement, work order, purchase order, or 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 Sub-Business Associate Agreement, and cure is not feasible, the non-breaching party may terminate this Sub-Business Associate Agreement immediately.

19. Disposition of Protected Health Information Upon Termination or Expiration

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

19.2 Destruction for purposes of Section 19.1 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 Contractor determines that any such Protected Health Information is necessary for Contractor to continue its proper management and administration or to carry out its legal responsibilities, Contractor may retain that Protected Health Information which is necessary for Contractor to continue its proper management and administration or to carry out its legal responsibilities and shall return or destroy all other Protected Health Information.

(a) Contractor shall extend the protections of this Sub-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 Contractor shall not Use or Disclose such Protected Health Information other than for the purposes for which such Protected Health Information was retained.

(b) Contractor shall return or, if agreed to by CalMHSA and Covered Entity, destroy the Protected Health Information retained by Contractor when it is no longer needed by Contractor for Contractor's proper management and administration or to carry out its legal responsibilities.

19.4 Contractor shall ensure that all Protected Health Information created, maintained, or received by Subcontractors is returned or, if agreed to by CalMHSA and Covered Entity, destroyed as provided for in Section 6.6.

20. Audit, Inspection, and Examination

20.1 CalMHSA and each Covered Entity Participant 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 of determining whether Contractor is in compliance with the terms of this Sub-Business Associate Agreement and any non-compliance may be a basis for termination of this Sub-Business Associate Agreement and the applicable underlying agreement, contract, master agreement, work order, purchase order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

20.2 CalMHSA and Contractor shall mutually agree in advance upon the scope, timing, and location of any such inspection.

20.3 At Contractor's request, and to the extent permitted by law, CalMHSA shall execute a nondisclosure agreement, upon terms and conditions mutually agreed to by the Parties.

20.4 CalMHSA's inspection, failure to inspect, or right to inspect as provided for in Section 20.1 does not relieve Contractor of its responsibility to comply with this Sub-Business Associate Agreement and/or the HIPAA Rules or impose on CalMHSA any responsibility for Contractor's compliance with any applicable HIPAA Rules.

20.5 CalMHSA's failure to detect, its detection but failure to notify Contractor, or its detection but failure to require remediation by Contractor of an unsatisfactory practice by Contractor, shall not constitute acceptance of such practice or a waiver of CalMHSA's enforcement rights under this Sub-Business Associate Agreement or the applicable underlying agreement, contract, master agreement, work order, purchase

order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

20.6 Section 20 is not intended by the Parties to limit in any way the scope of Contractor's obligations related to Inspection and/or Audit and/or similar review in the applicable underlying agreement, contract, master agreement, work order, purchase order, or other services arrangement, with or without payment, which gives rise to Contractor's status as a Business Associate.

21. Miscellaneous Sections

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

21.2 HIPAA Requirements. The Parties agree that the provisions under HIPAA Rules that are Required by Law to be incorporated into this Sub-Business Associate Agreement are hereby incorporated into the Contract.

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

21.4 Construction. In the event that a provision of this Sub-Business Associate Agreement is contrary to a provision of the Contract or any other applicable underlying agreement, contract, master agreement, work order, purchase order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, the provision of this Sub-Business Associate Agreement shall control. Otherwise, this Sub-Business Associate Agreement shall be construed under, and in accordance with, the terms of the Contract, with or without payment, that gives rise to Contractor's status as a Business Associate.

21.5 Regulatory References. A reference in this Sub-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 Sub-Business Associate Agreement shall be resolved in favor of a meaning that permits the Parties to comply with the HIPAA Rules.

21.7 Amendment. The Parties agree to take such action as is necessary to amend this Sub-Business Associate Agreement from time to time as is necessary for CalMHSA or Contractor to comply with the requirements of the HIPAA Rules and any other privacy laws governing Protected Health Information.

AUTHORIZED SIGNOR

CONTRACTOR: [CONTRACTOR NAME]

Signed:_____ Name (Printed): _____

Title:_____ Date:_____

Address: _____

Phone:_____ Email: _____

CONTRACTOR: CALIFORNIA MENTAL HEALTH SERVICES AUTHORITY (CalMHSA)

Signed:_____Name (Printed): Amie Miller, Psy.D., MFT

Title: Executive Director Date:_____

Address: 1610 Arden Way, Suite 175, Sacramento, CA 95815

Phone: (279) 234-0700 Email: amie.miller@calmhsa.org

DHCS Exhibit A

Exhibits H-1 and H-2

Privacy and Information Security Provisions

Exhibits A-1 and A-2 are intended to protect the privacy and security of specified DHCS information that Business Associate may access, receive, or transmit pursuant to either a Participation Agreement by and between CalMHSA and a Covered Entity Participant or the Restated Joint Exercise of Powers Agreement with an effective date of July 1, 2013 (the "JPA Agreement") (collectively each a "Participation Agreement") and that Contractor may subsequently access, receive, or transmit pursuant to the Contract. The DHCS information covered under this Exhibit A consists of: (1) PHI and (2) PI. PI may include data provided to DHCS by the Social Security Administration. For purposes of Exhibits H-1 and H-2, "Covered Entity" refers to CalMHSA, and "Business Associate" refers to Contractor.

DHCS Exhibit A consists of the following parts:

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

2. Exhibit A-2, Miscellaneous Provisions, sets forth additional terms and conditions that extend to the provisions of Exhibits H-1 and H-2 in their entirety.

Exhibit A-**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 A-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 applicable Participation Agreement and Contract. 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 A-1 shall apply.

c. The terms used in this Exhibit A-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 A-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 applicable Participation Agreement and Contract on behalf of the Covered Entity.

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

f. "Personally Identifiable Information" ("PII") shall have the meaning given to such term in the 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 applicable Participation Agreement and Contract; or interference with system operations in an information system that processes, maintains or stores Pl.

3. Terms of Agreement

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

3. Except as otherwise indicated in this Exhibit A-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 applicable Participation Agreement and Contract 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

4. Business Associate agrees:

i. **Nondisclosure**. Not to use or disclose DHCS PI or PII other than as permitted or

required by the applicable Participation Agreement and Contractor as required by applicable state and federal law.

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

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

i. Complying with all of the data system security precautions listed in Attachment A, Business 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 A-1.

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

f. **Availability of Information to Covered Entity and DHCS**. To make DHCS PI and PII available to Covered Entity or DHCS for purposes of oversight, inspection, amendment, and response to

requests for records, injunctions, judgments, and orders for production of DHCS PI and PII. If Business Associate receives DHCS PII, upon request by Covered Entity or DHCS, Business Associate shall provide Covered Entity or DHCS, as applicable, with a list of all employees, contractors and agents who have access to DHCS PII, including employees, contractors and agents of its subcontractors and agents.

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

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

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

    i. Initial Notice to Covered Entity. (1) To notify Covered Entity and DHCS immediately by telephone call or email or fax upon the discovery of a breach of unsecured DHCS PI or PII in electronic media or in any other media if the PI or PII was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon discovery of a suspected security incident involving DHCS PII. (2) To notify Covered Entity and DHCS within 24 hours by email or fax of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of DHCS PI or PII in violation of the applicable Participation Agreement and Contract or this Exhibit A-1 or potential loss of confidential data affecting the applicable Participation Agreement and Contract. 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.ca.gov), then select "Laws & Regulations" in the left column and then "Privacy" or use this link: https://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.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.

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 applicable Participation Agreement and Contract to which it is incorporated.

CalMHSA Privacy Officer	**Covered Entity Chief Privacy Officer**	**DHCS Privacy Officer**	**DHCS Information Security Officer**
Brandon Connors Privacy Officer Email: privacyofficer@calmhsa.org Telephone: (279) 202-7260	See the Business Associate Agreement for the applicable Covered Entity.	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

5. 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 A-1 and for communicating on security matters with Covered Entity and DHCS.

Exhibit A-**2**

Miscellaneous Terms and Conditions

Applicable to DHCS Exhibit A

1. **Disclaimer.** Covered Entity makes no warranty or representation that compliance by Business Associate with this DHCS Exhibit A, 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 DHCS Exhibit A 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 DHCS Exhibit A 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 Contract upon thirty (30) days written notice in the event:

    a. Business Associate does not promptly enter into this DHCS Exhibit A 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 Contract if Business Associate is found guilty of a criminal violation of HIPAA. Covered Entity may at the request of DHCS terminate the Contract 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 Contract.

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 applicable Participation Agreement and Contract, available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers or employees based upon

claimed violation of HIPAA, or the HIPAA regulations, which involves inactions or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named adverse party.

5. **No Third-Party Beneficiaries**. Nothing express or implied in the terms and conditions of this DHCS Exhibit A 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 DHCS Exhibit A 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 DHCS Exhibit A 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 Contract.

8. **Regulatory References**. A reference in the terms and conditions of this DHCS Exhibit A 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 A-1, Responsibilities of Business Associate, shall survive the termination or expiration of this Agreement.

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

11. **Audits, Inspection and Enforcement**. From time to time, and subject to all applicable federal and state privacy and security laws and regulations, Covered Entity or DHCS may conduct a reasonable inspection of the facilities, systems, books and records of to monitor compliance with this DHCS Exhibit A. Business Associate shall promptly remedy any violation of any provision of this DHCS Exhibit A. 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 DHCS Exhibit A. 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 applicable Participation Agreement and Contractor related documents, including this DHCS Exhibit A.

12. **Due Diligence**. Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this DHCS Exhibit A 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 DHCS Exhibit A.

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

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

Attachment A

Data Security Requirements

1. Personnel Controls

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

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

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

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

2. Technical Security Controls

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

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

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

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

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

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

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

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

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

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

3. Audit Controls

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

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

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

4. Business Continuity / Disaster Recovery Controls

a. **Emergency Mode Operation Plan**. Business Associate must establish a documented plan to enable continuation of critical business processes and protection of the security of DHCS PHI or PI held in an electronic format in the event of an emergency. Emergency

means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

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

5. Paper Document Controls

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

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

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