

**CALIFORNIA MENTAL HEALTH SERVICES AUTHORITY
PARTICIPATION AGREEMENT AMENDMENT
COVER SHEET**

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

Name of Services: Inter-Member Transfer(s)

2. This Participation Agreement Amendment extends the term of the initial Participation Agreement No. 421-2018-PT-FC and adds funding. All other provisions from the initial Participation Agreement No. 421-2018-PT—FC not cited in this Amendment shall remain in full force and effect.
3. **Term of Services:** This Agreement shall become effective upon execution and shall terminate on the 30th of June 2025.
5. The maximum amount payable under this Agreement Amendment is One Million Two Hundred Thousand and No/100 Dollars (**\$1,200,000**). CalMHSA shall invoice the Participant for the replenishment of funds and annual administrative fee not to exceed 5%. Any additional funding required in order to process transfer requests, shall be by mutual agreement of the parties followed by executing an Agreement Amendment.
6. Exhibit B of Initial Participation Agreement No. 421-2018-PT-FC is amended as follows:
1. Section II. Responsibilities, at Part A (7) is replaced with Business Associate Agreement below:

BUSINESS ASSOCIATE AGREEMENT

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

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

The HIPAA Rules require a written agreement ("Business Associate Agreement") between County and Contractor in order to mandate certain protections for the privacy and security of Protected Health

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

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

Therefore, the Parties agree as follows:

1. Definitions

- 1.1 "Breach" has the same meaning as the term "breach" at 45 C.F.R. § 164.402.
- 1.2 "Business Associate" has the same meaning as the term "business associate" at 45 C.F.R. § 160.103. For the convenience of the Parties, a "business associate" is a person or entity, other than a member of the workforce of covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to Protected Health Information. A "business associate" 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 CalMHSA 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 CalMHSA may Use Protected Health Information for de-identification of the information if de-identification of the information is required to provide Services.
- 2.3 CalMHSA may Use or Disclose Protected Health Information as Required by Law.
- 2.4 CalMHSA 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 CalMHSA 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 CalMHSA 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 CalMHSA 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 CalMHSA 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 CalMHSA 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 CalMHSA 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 CalMHSA 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 CalMHSA 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 CalMHSA shall report to Fresno County and all affected Covered Entity Participants any Use or Disclosure of Protected Health Information not permitted by this Sub-Business Associate Agreement, any 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) CalMHSA shall report to Fresno County and all affected Covered Entity Participants any Use or Disclosure of Protected Health Information by CalMHSA, its employees, representatives, agents or Subcontractors not provided for by the Contract of which CalMHSA becomes aware.
 - (b) CalMHSA shall report to Fresno County and all affected Covered Entity Participants any Security Incident of which CalMHSA becomes aware.
 - (c) CalMHSA shall report to Fresno County and all affected Covered Entity Participants any Breach by CalMHSA, its employees, representatives, agents, workforce members, or Subcontractors of Unsecured Protected Health Information that is known to CalMHSA or, by exercising reasonable diligence, would have been known to CalMHSA. CalMHSA 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 CalMHSA, 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, CalMHSA 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) CalMHSA shall make an immediate telephonic report upon discovery of the non-permitted Use or Disclosure of Protected Health Information, Security Incident or Breach of Unsecured Protected Health Information to the Business Systems Analyst 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) CalMHSA shall make a written report without unreasonable delay and in no event later than three (3) business days from the date of discovery by CalMHSA of the non-permitted Use or Disclosure of Protected Health Information, Security Incident, or Breach of Unsecured Protected Health Information and to the Business Systems Analyst, 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 CalMHSA 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 CalMHSA 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 CalMHSA 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 CalMHSA is not able to provide the information specified in this Section 5.2 at the time of the required report, CalMHSA shall provide such information promptly thereafter as such information becomes available.

5.3 CalMHSA may delay the notification required by this Section 5, if a Law Enforcement Official states to CalMHSA 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, CalMHSA shall delay its reporting and/or notification obligation(s) for the time period specified by the official.
- (b) If the statement is made orally, CalMHSA 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, CalMHSA shall ensure that any Subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of CalMHSA 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 CalMHSA with respect to such information.

- 6.2 CalMHSA 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, CalMHSA shall terminate, if feasible, any arrangement with Subcontractor by which Subcontractor creates, receives, maintains, or transmits Protected Health Information on behalf of CalMHSA.
- 6.4 If neither cure nor termination as set forth in Sections 6.2 and 6.3 is feasible, CalMHSA shall immediately notify Fresno County.
- 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 Fresno County 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 CalMHSA, any Protected Health Information created, received, maintained, or transmitted by Subcontractor on behalf of CalMHSA so as to enable CalMHSA to comply with the provisions of Section 19.
- 6.7 CalMHSA shall provide to Fresno County, at Fresno County'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 CalMHSA'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 CalMHSA's status as a Business Associate.

7. Access to Protected Health Information

- 7.1 To the extent Fresno County determines that Protected Health Information is maintained by CalMHSA or its agents or Subcontractors in a Designated Record Set, CalMHSA shall, within two (2) business days after receipt of a request from Fresno County, make the Protected Health Information specified by Fresno County available to the Individual(s) identified by Fresno County as being entitled to access and shall provide such Individual(s) or other person(s) designated by Fresno County with a copy the specified Protected Health Information, in order for Fresno County to meet the requirements of 45 C.F.R. § 164.524.
- 7.2 If any Individual requests access to Protected Health Information directly from CalMHSA or its agents or Subcontractors, CalMHSA shall notify Fresno County in writing within two (2) days of the receipt of the request. Whether access shall be provided or denied shall be determined by Fresno County.

- 7.3 To the extent that CalMHSA 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, CalMHSA 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 Fresno County and the Individual.

8. Amendment of Protected Health Information

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

9. Accounting of Disclosures of Protected Health Information

- 9.1 CalMHSA shall maintain an accounting of each Disclosure of Protected Health Information made by CalMHSA or its employees, agents, representatives or Subcontractors, as is determined by Fresno County to be necessary in order to permit Fresno County 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 CalMHSA 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, CalMHSA 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 CalMHSA shall provide to Fresno County, within ten (10) business days after receipt of a written request from Fresno County, information collected in accordance with Section 9.1

to permit Fresno County 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 CalMHSA or its agents or Subcontractors, CalMHSA shall notify Fresno County 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 CalMHSA is to carry out one or more of Fresno County's obligation(s) under Subpart E of 45 C.F.R. Part 164, CalMHSA shall comply with the requirements of Subpart E that apply to Fresno County's performance of such obligation(s).
- 10.2 CalMHSA shall comply with all HIPAA Rules applicable to CalMHSA in the performance of Services.

11. Availability of Records

- 11.1 CalMHSA 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 CalMHSA on behalf of Fresno County available to the Secretary for purposes of determining Fresno County's compliance with the Privacy and Security Regulations.
- 11.2 Unless prohibited by the Secretary, CalMHSA shall immediately notify Fresno County of any requests made by the Secretary and provide Fresno County with copies of any documents produced in response to such request.

12. Mitigation of Harmful Effects

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

13. Breach Notification to Individuals

- 13.1 CalMHSA shall, to the extent Fresno County determines that there has been a Breach of Unsecured Protected Health Information by CalMHSA, its employees, representatives, agents or Subcontractors, provide breach notification to the Individual in a manner that permits Fresno County to comply with its obligations under 45 C.F.R. § 164.404.
- (a) CalMHSA shall notify, subject to the review and approval of Fresno County 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 CalMHSA shall be written in plain language, shall be subject to review and approval by Fresno County 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 CalMHSA 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 CalMHSA shall reimburse Fresno County and each affected Covered Entity Participant any and all costs incurred by Fresno County, 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 CalMHSA's Breach of Unsecured Protected Health Information; Fresno County shall not be responsible for any costs incurred by CalMHSA in providing the notification required by 13.1 or in establishing the contact procedures required by Section 13.1.

14. DHCS Requirements.

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

15. Indemnification

- 15.1 CalMHSA shall indemnify, defend, and hold harmless Fresno County 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 CalMHSA'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 CalMHSA'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 CalMHSA's status as a Contractor.

16. Obligations of Fresno County

- 16.1 Fresno County shall notify CalMHSA of any current or future restrictions or limitations on the Use or Disclosure of Protected Health Information of which Fresno County is aware that would affect CalMHSA's performance of the Services, and CalMHSA shall thereafter restrict or limit its own Uses and Disclosures accordingly.
- 16.2 Fresno County shall not request CalMHSA 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 Fresno County or its Covered Entity Participants, except to the extent that CalMHSA 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 CalMHSA's status as a Contractor.
- 17.2 Notwithstanding Section 18, CalMHSA'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 CalMHSA'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 CalMHSA'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, CalMHSA shall return or, if agreed to by Covered entity, shall destroy as provided for in Section 19.2, all Protected Health Information received from Fresno County, or created, maintained, or received by CalMHSA on behalf of Fresno County and any Participant, that CalMHSA, including any Subcontractor, still maintains in any form. CalMHSA 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 CalMHSA determines that any such Protected Health Information is necessary for CalMHSA to continue its proper management and administration or to carry out its legal responsibilities, CalMHSA may retain that Protected Health Information which is necessary for CalMHSA 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) CalMHSA 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 CalMHSA shall not Use or Disclose such Protected Health Information other than for the purposes for which such Protected Health Information was retained.
- (b) CalMHSA shall return or, if agreed to by Fresno County and Covered entity, destroy the Protected Health Information retained by CalMHSA when it is no longer needed by CalMHSA for CalMHSA's proper management and administration or to carry out its legal responsibilities.

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

20. Audit, Inspection, and Examination

- 20.1 Fresno County 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 CalMHSA 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 CalMHSA's status as a Business Associate.
- 20.2 Fresno County and CalMHSA shall mutually agree in advance upon the scope, timing, and location of any such inspection.
- 20.3 At CalMHSA's request, and to the extent permitted by law, Fresno County shall execute a nondisclosure agreement, upon terms and conditions mutually agreed to by the Parties.
- 20.4 Fresno County's inspection, failure to inspect, or right to inspect as provided for in Section 20.1 does not relieve CalMHSA of its responsibility to comply with this Sub-Business Associate Agreement and/or the HIPAA Rules or impose on Fresno County any responsibility for CalMHSA's compliance with any applicable HIPAA Rules.
- 20.5 Fresno County's failure to detect, its detection but failure to notify CalMHSA, or its detection but failure to require remediation by CalMHSA of an unsatisfactory practice by CalMHSA, shall not constitute acceptance of such practice or a waiver of Fresno County'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 CalMHSA's status as a Business Associate.
- 20.6 Section 20 is not intended by the Parties to limit in any way the scope of CalMHSA'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 CalMHSA's status as a Business Associate.

21. Miscellaneous Sections

- 21.1 Disclaimer. Fresno County makes no warranty or representation that compliance by CalMHSA 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 CalMHSA.

- 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 CalMHSA'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 CalMHSA'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 CalMHSA to comply with the requirements of the HIPAA Rules and any other privacy laws governing Protected Health Information.

DHCS Exhibit A

Exhibits A-1 and A-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 under the JPA Agreement. 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 A-1 and A-2, "Covered Entity" refers to Fresno County, and "Business Associate" refers to CalMHSA.

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 A-1 and A-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 JPA Agreement. Specifically this Exhibit applies to PI and PII which is not PHI as defined by HIPAA and therefore is not addressed in this Business Associate Agreement; however, to the extent that data is both PHI or ePHI and PII, both the Business Associate Agreement and this Exhibit 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 JPA Agreement on behalf of the Covered Entity.
- e. "Notice-triggering Personal Information" shall mean the personal information identified in Civil Code section 1798.29 whose unauthorized access may trigger notification requirements under Civil Code section 1798.29. For purposes of this provision, identity shall include, but not

be limited to, name, address, email address, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, a photograph or a biometric identifier. Notice-triggering Personal Information includes PI in electronic, paper or any other medium.

- f. "Personally Identifiable Information" ("PII") shall have the meaning given to such term in the CMPPA.
- g. "Personal Information" ("PI") shall have the meaning given to such term in California Civil Code Section 1798.3(a).
- h. "Required by law" means a mandate contained in law that compels an entity to make a use or disclosure of PI or PII that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- i. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PI, or confidential data utilized in complying with the JPA Agreement; or interference with system operations in an information system that processes, maintains or stores PI.

3. Terms of Agreement

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

- 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 JPA Agreement provided that such use or disclosure would not violate the California Information Practices Act ("CIPA") if done by the DHCS.

b. Responsibilities of Business Associate

- 4. Business Associate agrees:
 - i. **Nondisclosure.** Not to use or disclose DHCS PI or PII other than as permitted or required by the JPA Agreement or as required by applicable state and federal law.
 - ii. **Safeguards.** To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of DHCS PI and PII, to protect against anticipated threats or hazards to the security or integrity of DHCS PI and PII, and to prevent use or disclosure of DHCS PI or PII other than as provided for by the JPA Agreement. Business Associate shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Business

Associate's operations and the nature and scope of its activities, which incorporate the requirements of section (c), Security, below. Business Associate will provide Covered Entity or DHCS with its current policies upon request.

- c. **Security.** Business Associate shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:
 - i. Complying with all of the data system security precautions listed in Attachment A, Business Associate Data Security Requirements;
 - ii. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and
 - iii. If the data obtained by Business Associate from DHCS through Covered Entity includes PII, Contractor shall also comply with the substantive privacy and security requirements in the CMPPA Agreement. Business Associate also agrees to ensure that any agents, including a subcontractor to whom it provides DHCS PII, agree to the same requirements for privacy and security safeguards for confidential data that apply to Business Associate with respect to such information.
- d. **Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of DHCS PI or PII by Business Associate or its subcontractors in violation of this Exhibit 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 JPA Agreement that involve the disclosure of DHCS PI or PII to the subcontractor.
- f. **Availability of Information to Covered Entity and DHCS.** To make DHCS PI and PII available to Covered Entity or DHCS for purposes of oversight, inspection, amendment, and response to requests for records, injunctions, judgments, and orders for production of DHCS PI and PII. If Business Associate receives DHCS PII, upon request by Covered Entity or DHCS, Business Associate shall provide Covered Entity or DHCS, as applicable, with a list of all employees, contractors and agents who have access to DHCS PII, including employees, contractors and agents of its subcontractors and agents.
- g. **Cooperation with Covered Entity and DHCS.** With respect to DHCS PI, to cooperate with and assist the Covered Entity or DHCS, as applicable, to the extent necessary to ensure DHCS's compliance with the applicable terms of the CIPA including, but not limited to, accounting of disclosures of DHCS PI, correction of errors in DHCS PI, production of DHCS PI, disclosure of a security breach involving DHCS PI and notice of such breach to the affected individual(s).
- h. **Confidentiality of Alcohol and Drug Abuse Patient Records.** Business Associate agrees to comply with all confidentiality requirements set forth in Title 42 Code of Federal Regulations,

Chapter I, Subchapter A, Part 2. Business Associate is aware that criminal penalties may be imposed for a violation of these confidentiality requirements.

- i. **Breaches and Security Incidents.** During the term of this Agreement, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:
 - i. Initial Notice to Covered Entity. (1) To notify Covered Entity and DHCS immediately by telephone call or email or fax upon the discovery of a breach of unsecured DHCS PI or PII in electronic media or in any other media if the PI or PII was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon discovery of a suspected security incident involving DHCS PII. (2) To notify Covered Entity and DHCS within 24 hours by email or fax of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of DHCS PI or PII in violation of the JPA Agreement or this Exhibit A-1 or potential loss of confidential data affecting the JPA Agreement. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.
 - ii. Notice shall be provided to the Covered Entity Chief Privacy Officer and DHCS Information Protection Unit, Office of HIPAA Compliance. If the incident occurs after business hours or on a weekend or holiday and involves electronic DHCS PI or PII, notice shall be provided to DHCS by calling the DHCS Information Security Officer. Notice to DHCS shall be made using the DHCS "Privacy Incident Report" form, including all information known at the time. Business Associate shall use the most current version of this form, which is posted on the DHCS Information Security Officer website (www.dhcs.camgov, then select "Privacy" in the left column and then "Business Partner" near the middle of the page) or use this link: <http://www.dhcs.ca.gov/formsandoubs/laws/oriv/Paces/DHCSBusinessAssociatesOnlv.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 JPA Agreement to which it is incorporated.

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

j. Designation of Individual Responsible for Security

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 H

1. **Disclaimer.** Covered Entity makes no warranty or representation that compliance by Business Associate with this DHCS Exhibit H, 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 H 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 H embodying written assurances consistent with requirements of HIPAA, the HITECH Act, and the HIPAA regulations, and other applicable state and federal laws. Covered Entity may terminate the JPA Agreement upon thirty (30) days written notice in the event:
 - a. Business Associate does not promptly enter into this DHCS Exhibit H when requested by Covered Entity; or
 - b. Business Associate does not enter into an amendment providing assurances regarding the safeguarding of DHCS PHI that the DHCS deems is necessary to satisfy the standards and requirements of HIPAA and the HIPAA regulations
3. **Judicial or Administrative Proceedings.** Business Associate will notify Covered Entity and DHCS if it is named as a defendant in a criminal proceeding for a violation of HIPAA or other security or privacy law. Covered Entity may at the request of DHCS terminate the JPA Agreement if Business Associate is found guilty of a criminal violation of HIPAA. Covered Entity may at the request of DHCS terminate the JPA Agreement if a finding or stipulation that Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined. DHCS will consider the nature and seriousness of the violation in deciding whether or not to request that Covered Entity terminate the JPA Agreement.
4. **Assistance in Litigation or Administrative Proceedings.** Business Associate shall make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under the JPA Agreement, available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers or employees based upon claimed violation of HIPAA, or the HIPAA regulations, which involves inactions or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named adverse party.
5. **No Third-Party Beneficiaries.** Nothing express or implied in the terms and conditions of this DHCS Exhibit H 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 H 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 H shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations, and, if applicable, any other relevant state and federal laws.
7. **Conflict.** In case of a conflict between any applicable privacy or security rules, laws, regulations or standards the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI, PI and PII from unauthorized disclosure. Further, Business Associate must comply within a reasonable period of time with changes to these standards that occur after the effective date of the JPA Agreement.
8. **Regulatory References.** A reference in the terms and conditions of this 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 JPA Agreement or 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 H 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 PI. The statement must be renewed annually. Business Associate shall retain each person's written confidentiality statement for Covered Entity or DHCS inspection for a period of six (6) years following termination of this Agreement.
- d. **Background Check.** Before a member of the workforce may access DHCS PHI or PI, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. Business Associate shall retain each workforce member's background check documentation for a period of three (3) years.

2. Technical Security Controls

- a. **Workstation/Laptop encryption.** All workstations and laptops that store DHCS PHI or PI either directly or temporarily must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DHCS Information Security Office.
- b. **Server Security.** Servers containing unencrypted DHCS PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- c. **Minimum Necessary.** Only the minimum necessary amount of DHCS PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.
- 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 username 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 PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If DHCS PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.
- p. **Access Controls.** The system providing access to DHCS PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.
- q. **Transmission encryption.** All data transmissions of DHCS PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing DHCS PHI can be encrypted. This requirement pertains to any type of DHCS PHI or PI in motion such as website access, file transfer, and E-Mail.
- r. **Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting DHCS PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. Audit Controls

- a. **System Security Review.** Business Associate must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing DHCS PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.
- b. **Log Reviews.** All systems processing and/or storing DHCS PHI or PI must have a routine procedure in place to review system logs for unauthorized access.
- c. **Change Control.** All systems processing and/or storing DHCS PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4. Business Continuity / Disaster Recovery Controls

- a. **Emergency Mode Operation Plan.** Business Associate must establish a documented plan to enable continuation of critical business processes and protection of the security of DHCS PHI or PI held in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.
- b. **Data Backup Plan.** Business Associate must have established documented procedures to backup DHCS PHI to maintain retrievable exact copies of DHCS PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DHCS PHI or PI

April 7, 2022

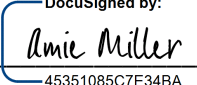
should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

5. Paper Document Controls

- a. **Supervision of Data.** DHCS PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DHCS PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
- b. **Escorting Visitors.** Visitors to areas where DHCS PHI or PI is contained shall be escorted and DHCS PHI or PI shall be kept out of sight while visitors are in the area.
- c. **Confidential Destruction.** DHCS PHI or PI must be disposed of through confidential means, such as crosscut shredding and pulverizing.
- 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.

7. Authorized Signatures:

CalMHSA

Signed:  Name (Printed): Amie Miller, Psy.D., MFT
45351085C7E34BA...
Title: Executive Director Date: 5/12/2022

Participant: Fresno County

Signed: See Attached Signature Page Name (Printed): _____
Title: _____ Date: _____

April 7, 2022

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year first hereinabove written.

CONTRACTOR:

COUNTY OF FRESNO

See Previous Signature Page

(Authorized Signature)



Brian Pacheco,
Chairman of the Board of Supervisors
of the County of Fresno

Print Name & Title

Mailing Address

ATTEST:

Bernice E. Seidel
Clerk of the Board of Supervisors
County of Fresno, State of California

By:



Deputy

FOR ACCOUNTING USE ONLY:

Fund/Subclass: 0001/10000

Organization: 56302005

Account #: 7295