



Tehama County Minutes Certification

File Number: 25-0494

Enactment Number: MISC. AGR 2025-070

11. HEALTH SERVICES AGENCY / MENTAL HEALTH 25-0494

a) AGREEMENT - Approval and authorization for the Executive Director to sign Agreement #12388-TC-Peers with the California Mental Health Services Authority (CalMHSA) for participation in the Medi-Cal Peer Support Specialist Certification program, effective upon the date of execution and shall terminate one year from execution.

Enactment No: MISC. AGR 2025-070

Approval of the Consent Agenda.

A motion was made by Supervisor Jones, seconded by Supervisor Walker, to approve the Consent Agenda. The motion carried by the following vote:

- RESULT:** APPROVED THE CONSENT AGENDA
- MOVER:** Greg Jones
- SECONDER:** Tom Walker
- AYES:** Supervisor Jones, Supervisor Burroughs, Supervisor Walker, and Chairperson Hansen
- ABSENT:** Vice Chair Nolen

I, SEAN HOUGHTBY, County Clerk and ex-officio Clerk of the Board of Supervisors of the County of Tehama, State of California, hereby certify the above and foregoing to be a full, true and correct copy of an order adopted by said Board of Supervisors on 4/8/2025.

Attest: 
Deputy

April 11, 2025
Date Certified

CALIFORNIA MENTAL HEALTH SERVICES AUTHORITY

PARTICIPATION AGREEMENT
MEDI-CAL PEER SUPPORT SPECIALIST CERTIFICATION PROGRAM

COVER SHEET

Tehama County ("Participant") desires to participate in the Medi-Cal Peer Support Specialist Certification Program ("Program") offered by the California Mental Health Services Authority ("CalMHSA") on the terms provided in this Participation Agreement ("Agreement"). Participant acknowledges that the Program also will be governed by CalMHSA's Joint Powers Agreement and its Bylaws. The Agreement is effective upon the date of final signature by both parties through one year from the effective date ("Term"). The following exhibits are attached and form part of this Agreement:

- Attachment A Detailed Program Description, Requirements, Restrictions
- Attachment B General Terms and Conditions
- Attachment C JPA-BAA

1. **Summary of Program:** CalMHSA is offering the following Program to Counties:

The Medi-Cal Peer Support Specialist Certification Program supports Counties in implementing the optional Medi-Cal Peer Support benefit in accordance with Department of Health Care Services ("DHCS") Behavioral Health Information Notice 21-041. CalMHSA represents Counties in the development of a uniform peer certification program that meets state requirements. For the development of the peer certification program, CalMHSA has established a uniform process that supports county reciprocity for certification. This Agreement acknowledges the Participant's involvement in this program and defines CalMHSA's role in providing Program data to the Participant on an ongoing basis.

Authorized Signatures:

CalMHSA

DocuSigned by:
 Signed: Dr. Amie Miller Name (Printed): Dr. Amie Miller, Psy.D., MFT
82E9EFBAB7CC446...
 Title: Executive Director Date: 4/23/2025

Participant: TEHAMA COUNTY

Signed: Jayne S. Bottke Name (Printed): Jayne S. Bottke
 Title: Executive Director Date: 3-21-25

Participation Agreement
Attachment A – Detailed Program Description, Obligations, Restrictions

Detailed Program Description:

The Medi-Cal Peer Support Specialist Certification Program supports Counties in implementing the optional Medi-Cal Peer Support benefit in accordance with Department of Health Care Services (“DHCS”) [Behavioral Health Information Notice 21-041](#) and updated BHIIN guidance. CalMHSA represents Counties in the development of a uniform peer certification program that meets state requirements. For the development of the peer certification program, CalMHSA has established a uniform process that supports county reciprocity for certification.

CalMHSA is the certifying entity (“Certifying Entity”) for Medi-Cal Peer Support Specialists. As the Certifying Entity, CalMHSA is responsible for the administrative functions of the Program. To this end, CalMHSA has established a dedicated certification website (“Website”) for information about certification in California (See capeercertification.org), the development of a Certification Portal (“Portal”) anchored to the Website that allows candidates to apply for certification through the Website. The Portal is instrumental in aiding CalMHSA in the collection of candidate information necessary for ensuring each candidate meets certification standards, issuing of certification, and the collection of candidate data used for program evaluation and annual reporting required set by the DHCS. Additionally, CalMHSA is responsible for the enforcement of professional standards for certification, maintaining the public-facing certification registry (“Certification Registry”), the approval of training providers, and administration of the examination for certification. Lastly, CalMHSA is responsible for conducting investigations for allegations made against a certified professional for legal and ethical violations (based on the established [Code of Ethics](#)).

Obligations:

CalMHSA shall:

- Perform administrative activities as the Certifying Entity, including, but not limited to:
 - Maintenance of the certification website (capeercertification.org);
 - Maintenance of the Portal, and an on-line application for certification;
 - Process applications to ensure candidates meet certification standard and issue certification;
 - Collect candidate information for Program evaluation and annual data reporting as required by the DHCS.
 - Enforce professional standards for certification, including conducting investigations for allegations made against a certified professional for legal and ethical violations (See [Code of Ethics](#)).
 - Maintenance of the Certification Registry;
 - Administration and scoring of the certification examination; and
 - Approve training providers.

- Maintain current [Guidelines, Standards, and Procedure Manual for Medi-Cal Peer Support Specialist Certification](#) program.
- Apply continuous quality improvement principles to evaluate Program performance.
- Conduct quality assurance reviews of CalMHSA-approved training providers to ensure quality training.
- Maintain centralized, searchable, and publicly accessible Certification Registry.
- Compile and submit data to meet state reporting requirements, in accordance with DHCS BHINs.
- Compile and submit the following state reporting data regarding active and pending applications and certifications and send to Participants upon request via a secure DropBox link. The data request may be subject to change based on the requirements set forth by DHCS in subsequent BHINs.
 - First Name
 - Middle Name
 - Last Name
 - Application Status
 - Scholarship Status
 - Email
 - Number Of Peer Support Specialists Certified
 - Number Of Applicants That Did Not Receive Certification
 - Number Of Applicants Employed in Peer Services Prior To Certification
 - Number Of Applicants Certified in an Area of Specialization
 - Number of Certified Peers That Renewed Certification
 - Number Of Peer Supervisor Trainings Provided
 - Number of Applicants that received Certification through Grandparenting Process
 - Number Of Applicants that received Certification through State Reciprocity
 - Peer Support Specialist Demographics-Age, Gender identity, Race/ethnicity, Proficient Language
 - Number of applicants that applied for Medi-Cal Peer Support Specialist Certification through Grandparenting process
 - Data visualization of certification history over time for previous FYs.
 - Status/Health of the Program: Complaints and/or corrective actions against certified individuals

Participant shall:

- Accept files from CalMHSA using designated secure file transfer.
- Communicate all questions and concerns to CalMHSA via workforce@calmhsa.org.

Program Restrictions:

- Timelines and technical requirements may need adjusting due to unique circumstances.

Participation Agreement
Attachment B - General Terms and Conditions

I. Definitions

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

- A.** CalMHSA – California Mental Health Services Authority, a Joint Powers Authority (JPA) created by counties in 2009 at the instigation of the California Mental Health Directors Association to jointly develop and fund mental health services and education programs.
- B.** Member – A County (or JPA of two or more Counties) that has joined CalMHSA and executed the CalMHSA Joint Powers Agreement.
- C.** Participant – Any County participating in the Program either as Member of CalMHSA or under a Memorandum of Understanding with CalMHSA.
- D.** Program – The program identified in the Cover Sheet offered by CalMHSA under the Agreement.

II. Responsibilities

- A.** Responsibilities of CalMHSA:
 - 1. Provide the Program as described in the Agreement;
 - 2. Act as the Fiscal and Administrative agent for the Program.
 - 3. Comply with CalMHSA's Joint Powers Agreement and Bylaws.
- B.** Responsibilities of Participant:
 - 1. Provide CalMHSA and any other parties deemed necessary with requested information and assistance to fulfill the purpose of the Program.
 - 2. Cooperate by providing CalMHSA with requested information and assistance to fulfill the purpose of the Program.
 - 3. Provide feedback on Program performance.
 - 4. Comply with applicable laws, regulations, guidelines, contractual agreements, JPA requirements, and bylaws.

- III. Amendment.** This Agreement may be supplemented, amended, or modified only by the mutual agreement of CalMHSA and the Participant, expressed in writing and signed by an authorized representative of both parties.

IV. Withdrawal, Cancellation, and Termination

- A.** Participant may withdraw from the Program and terminate the Agreement upon six (6) months' written notice to CalMHSA. Notice shall be deemed served on the date of mailing.
- B.** Member Cost Sharing. The withdrawal of a Participant from the Program shall not automatically terminate its responsibility for its share of the expense and liabilities of

the Program. The contributions of current and past Participants are chargeable for their share of unavoidable expenses and liabilities arising during their participation period.

- C. CalMHSA may terminate, cancel, change, or limit the Program due to circumstances, including but not limited to, lack of County participation, government restrictions, issues with vendors or their services/platforms/products, lack of funding, governmental funding changes, inability to provide the Program due to vendor(s), regulatory changes, force majeure, or other issues.
- D. If applicable, upon cancellation, termination, or other conclusion of the Program, any funds remaining undisbursed after CalMHSA satisfies all obligations arising under the Program shall be returned to Participant. However, funds used to pay for completed deliverables, services rendered, upfront fees to create the Program, or fees for any portal or platform, ongoing services etc. are not subject to such reversion (subject to applicable laws). Unused funds that were paid for by a joint effort will be returned pro rata to Participant in proportion to payments made. Adjustments may be made if disproportionate benefit was conveyed to a particular Participant. Excess funds at the conclusion of county-specific efforts will be returned to the particular County that paid them per the Program.

V. Indemnification

- A. **Indemnification.** To the fullest extent permitted by law, each party shall hold harmless, defend and indemnify the other party, including its governing board, employees and agents from and against any and all claims, losses, damages, liabilities, disallowances, recoupments, and expenses, including but not limited to reasonable attorney's fees, arising out of or resulting from the indemnifying party's negligence or willful conduct in the performance of its obligations under this Agreement, including the performance of the other's subcontractors, except that each party shall have no obligation to indemnify the other for damages to the extent resulting from the negligence or willful misconduct of any indemnitee. Each party may participate in the defense of any such claim without relieving the other of any obligation hereunder.
- B. **No Responsibility for Mental Health Services.** CalMHSA is not undertaking responsibility for assessments, creation of case or treatment plans, providing or arranging services, and/or selecting, contracting with, or supervising providers (collectively, "mental health services"). Participant will defend and indemnify CalMHSA for any claim, demand, disallowance, suit, or damages arising from Participant's acts or omissions in connection with the provision of mental health services.

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

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

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

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

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

Therefore, the parties agree as follows:

1. DEFINITIONS

- 1.1 "Breach" has the same meaning as the term "breach" at 45 C.F.R. § 164.402.
- 1.2 "Business Associate" has the same meaning as the term "business associate" at 45 C.F.R. § 160.103. For the convenience of the parties, a "business associate" is a person or entity, other than a member of the workforce of covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to Protected Health Information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of another business associate. And in reference to the party to this Business Associate Agreement "Business Associate" shall mean Contractor.

- 1.3 "California Confidentiality Laws" means the applicable laws of the State of California governing the confidentiality, privacy, or security of PHI or other PII, including, but not limited to, the California Confidentiality of Medical Information Act (Cal. Civil Code § 56 et seq.), the patient access law (Cal. Health & Safety Code § 123100 et seq.), the HIV test result confidentiality law (Cal. Health & Safety Code § 120975 et seq.), the Lanterman-Petris-Short Act (Cal. Welf. & Inst. Code § 5328 et seq.), and California's data breach law (Cal. Civil Code § 1798.29).
- 1.4 "Covered Entity" has the same meaning as the term "covered entity" at 45 C.F.R. § 160.103, and in reference to the party to this Business Associate Agreement, "Covered Entity" shall mean County.
- 1.5 "Data Aggregation" has the same meaning as the term "data aggregation" at 45 C.F.R. § 164.501.
- 1.6 "De-identification" refers to the de-identification standard at 45 C.F.R. § 164.514.
- 1.7 "Designated Record Set" has the same meaning as the term "designated record set" at 45 C.F.R. § 164.501.
- 1.8 "Disclose" and "Disclosure" mean, with respect to Protected Health Information, the release, transfer, provision of access to, or divulging in any other manner of Protected Health Information outside Business Associate's internal operations or to other than its workforce. (See 45 C.F.R. § 160.103.)
- 1.9 "Electronic Health Record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. (See 42 U.S. C. § 17921.)
- 1.10 "Electronic Media" has the same meaning as the term "electronic media" at 45 C.F.R. § 160.103. For the convenience of the parties, electronic media means (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.
- 1.11 "Electronic Protected Health Information" has the same meaning as the term "electronic protected health information" at 45 C.F.R. § 160.103, limited to Protected Health Information created or received by Business Associate from or on behalf of Covered Entity. For the

convenience of the parties, Electronic Protected Health Information means Protected Health Information that is (i) transmitted by electronic media; (ii) maintained in electronic media.

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

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

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

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

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

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

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

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

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

- 1.21 "Subcontractor" has the same meaning as the term "subcontractor" at 45 C.F.R. § 160.103.
- 1.22 "Unsecured Protected Health Information" has the same meaning as the term "unsecured protected health information" at 45 C.F.R. § 164.402.
- 1.23 "Use" or "Uses" means, with respect to Protected Health Information, the sharing, employment, application, utilization, examination or analysis of such Information within Business Associate's internal operations. (See 45 C.F.R § 164.103.)
- 1.24 Terms used, but not otherwise defined in this Business Associate Agreement, have the same meaning as those terms in the HIPAA Rules.

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

- 2.1 Business Associate may only Use and/or Disclose Protected Health Information as necessary to perform Services, and/or as necessary to comply with the obligations of this Business Associate Agreement.
- 2.2 Business Associate may Use Protected Health Information for de-identification of the information if de-identification of the information is required to provide Services.
- 2.3 Business Associate may Use or Disclose Protected Health Information as Required by Law.
- 2.4 Business Associate shall make Uses and Disclosures and requests for Protected Health Information consistent with the Covered Entity's applicable Minimum Necessary policies and procedures.
- 2.5 Business Associate may Use Protected Health Information as necessary for the proper management and administration of its business or to carry out its legal responsibilities.
- 2.6 Business Associate may Disclose Protected Health Information as necessary for the proper management and administration of its business or to carry out its legal responsibilities, provided the Disclosure is Required by Law or Business Associate obtains reasonable assurances from the person to whom the Protected Health Information is disclosed (i.e., the recipient) that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purposes for which it was disclosed to the recipient and the recipient notifies Business Associate of any instances of which it is aware in which the confidentiality of the Protected Health Information has been breached.

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

3. PROHIBITED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

- 3.1 Business Associate shall not Use or Disclose Protected Health Information other than as permitted or required by this Business Associate Agreement or as Required by Law.
- 3.2 Business Associate shall not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164, or the California Confidentiality Laws if done by Covered Entity, except for the specific Uses and Disclosures set forth in Sections 2.5 and 2.6.
- 3.3 Business Associate shall not Use or Disclose Protected Health Information for de-identification of the information except as set forth in section 2.2.

4. OBLIGATIONS TO SAFEGUARD PROTECTED HEALTH INFORMATION

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

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

- 5.1 Business Associate shall report to Covered Entity any Use or Disclosure of Protected Health Information not permitted by this Business Associate Agreement, any Security Incident, and/or any Breach of Unsecured Protected Health Information as further described in Sections 5.1.1, 5.1.2, and 5.1.3.
- 5.1.1 Business Associate shall report to Covered Entity any Use or Disclosure of Protected Health Information by Business Associate, its employees, representatives, agents or Subcontractors not provided for by this Agreement of which Business Associate becomes aware.
- 5.1.2 Business Associate shall report to Covered Entity any Security Incident of which

Business Associate becomes aware.

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

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

5.2.1 Business Associate shall make an immediate telephonic report upon discovery of the non-permitted Use or Disclosure of Protected Health Information, Security Incident or Breach of Unsecured Protected Health Information to **(530) 527-8491 ext. 3991** that minimally includes:

- (a) A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident, or Breach and the date of Discovery of the non-permitted Use or Disclosure, Security Incident, or Breach, if known;
- (b) The number of Individuals whose Protected Health Information is involved;
- (c) A description of the specific type of Protected Health Information involved in the non-permitted Use or Disclosure, Security Incident, or Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);
- (d) The name and contact information for a person highly knowledgeable of the facts and circumstances of the non-permitted Use or Disclosure of PHI, Security Incident, or Breach.

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

Compliance Officer at:

Compliance Officer
Tehama County Health Services Agency, Mental Health
P.O. Box 400, Red Bluff, CA 96080
complianceofficer@tchsa.net

that includes, to the extent possible:

- (a) A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident, or Breach and the date of Discovery of the non-permitted Use or Disclosure, Security Incident, or Breach, if known;
- (b) The number of Individuals whose Protected Health Information is involved;
- (c) A description of the specific type of Protected Health Information involved in the non-permitted Use or Disclosure, Security Incident, or Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);
- (d) The identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, Used, or Disclosed;
- (e) Any other information necessary to conduct an assessment of whether notification to the Individual(s) under 45 C.F.R. § 164.404 is required;
- (f) Any steps Business Associate believes that the Individual(s) could take to protect him or herself from potential harm from the non-permitted Use or Disclosure, Security Incident, or Breach;
- (g) A brief description of what Business Associate is doing to investigate, to mitigate harm to the Individual(s), and to protect against any further similar occurrences; and
- (h) The name and contact information for a person highly knowledgeable of the facts and circumstances of the non-permitted Use or Disclosure of PHI, Security Incident, or Breach.

5.2.3 If Business Associate is not able to provide the information specified in Section

5.2.1 or 5.2.2 at the time of the required report, Business Associate shall provide such information promptly thereafter as such information becomes available.

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

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

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

6. WRITTEN ASSURANCES OF SUBCONTRACTORS

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

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

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

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

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

- 6.6 Without limiting the requirements of Section 6.1, agreement required by Section 6.1 (Subcontractor Business Associate Agreement) shall include a provision requiring Subcontractor to destroy, or in the alternative to return to Business Associate, any Protected Health Information created, received, maintained, or transmitted by Subcontractor on behalf of Business Associate so as to enable Business Associate to comply with the provisions of Section 18.4.
- 6.7 Business Associate shall provide to Covered Entity, at Covered Entity's request, a copy of any and all Subcontractor Business Associate Agreements required by Section 6.1.
- 6.8 Sections 6.1 and 6.7 are not intended by the parties to limit in any way the scope of Business Associate's obligations related to Subcontracts or Subcontracting in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

7. ACCESS TO PROTECTED HEALTH INFORMATION

- 7.1 To the extent Covered Entity determines that Protected Health Information is maintained by Business Associate or its agents or Subcontractors in a Designated Record Set, Business Associate shall, within two (2) business days after receipt of a request from Covered Entity, make the Protected Health Information specified by Covered Entity available to the Individual(s) identified by Covered Entity as being entitled to access and shall provide such Individuals(s) or other person(s) designated by Covered Entity with a copy the specified Protected Health Information, in order for Covered Entity to meet the requirements of 45 C.F.R. § 164.524 or the California Confidentiality Laws.
- 7.2 If any Individual requests access to Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within two (2) days of the receipt of the request. Whether access shall be provided or denied shall be determined by Covered Entity.
- 7.3 To the extent that Business Associate maintains Protected Health Information that is subject to access as set forth above in one or more Designated Record Sets electronically and if the Individual requests an electronic copy of such information, Business Associate shall provide the Individual with access to the Protected Health Information in the electronic form and format requested by the Individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by Covered Entity and the Individual.

8. AMENDMENT OF PROTECTED HEALTH INFORMATION

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

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

9. ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

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

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

- (a) The date of the Disclosure;
- (b) The name, and address if known, of the entity or person who received the Protected Health Information;
- (c) A brief description of the Protected Health Information Disclosed; and
- (d) A brief statement of the purpose of the Disclosure.

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

9.2 Business Associate shall provide to Covered Entity, within ten (10) business days after receipt of a written request from Covered Entity, information collected in accordance with Section

9.1.1 to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528

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

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

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

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

11. AVAILABILITY OF RECORDS

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

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

12. MITIGATION OF HARMFUL EFFECTS

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

13. BREACH NOTIFICATION TO INDIVIDUALS

13.1 Business Associate shall, to the extent Covered Entity determines that there has been a Breach of Unsecured Protected Health Information by Business Associate, its employees, representatives, agents or Subcontractors, provide breach notification to the Individual in a

manner that permits Covered Entity to comply with its obligations under 45 C.F.R. § 164.404.

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

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

- (a) A brief description of what happened, including the date of the Breach and the date of the Discovery of the Breach, if known;
- (b) A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- (c) Any steps the Individual should take to protect him or herself from potential harm resulting from the Breach;
- (d) A brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to Individual(s), and to protect against any further Breaches; and
- (e) Contact procedures for Individual(s) to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

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

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

14. DHCS REQUIREMENTS.

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

15. INDEMNIFICATION

15.1 Business Associate shall indemnify, defend, and hold harmless Covered Entity, its Special Districts, elected and appointed officers, employees, and agents from and against any and all liability, including but not limited to demands, claims, actions, fees, costs, expenses (including attorney and expert witness fees), and penalties and/or fines (including regulatory penalties and/or fines), arising from or connected with Business Associate's acts and/or omissions arising from and/or relating to this Business Associate Agreement, including, but not limited to, compliance and/or enforcement actions and/or activities, whether formal or informal, by the Secretary or by the Attorney General of the State of California.

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

16. OBLIGATIONS OF COVERED ENTITY

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

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

17. TERM

17.1 Unless sooner terminated as set forth in Section 18, the term of this Business Associate Agreement shall be the same as the term of the applicable underlying Agreement, Contract,

Participation Agreement, Master Agreement, Work Order, Purchase Order, or other service arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate. Such term shall apply to all such agreements entered into from time to time between the parties for the purpose of providing Services pursuant to the JPA.

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

18. TERMINATION FOR CAUSE

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

18.2 In addition to and notwithstanding the termination provisions set forth in the applicable underlying Agreement, Contract, Participation Agreement, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, if either party determines that the other party has violated a material term of this Business Associate Agreement, and cure is not feasible, the non-breaching party may terminate this Business Associate Agreement immediately.

19. DISPOSITION OF PROTECTED HEALTH INFORMATION UPON TERMINATION OR EXPIRATION

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

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

19.3 Notwithstanding Section 19.1, in the event that return or destruction of Protected Health

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

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

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

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

20. AUDIT, INSPECTION, AND EXAMINATION

20.1 Covered Entity reserves the right to conduct a reasonable inspection of the facilities, systems, information systems, books, records, agreements, and policies and procedures relating to the Use or Disclosure of Protected Health Information for the purpose determining whether Business Associate is in compliance with the terms of this Business Associate Agreement and any non-compliance may be a basis for termination of this Business Associate Agreement and the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, as provided for in section 18.

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

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

parties.

- 20.4 That Covered Entity inspects, fails to inspect, or has the right to inspect as provided for in Section 20.1 does not relieve Business Associate of its responsibility to comply with this Business Associate Agreement and/or the HIPAA Rules or impose on Covered Entity any responsibility for Business Associate's compliance with any applicable HIPAA Rules.
- 20.5 Covered Entity's failure to detect, its detection but failure to notify Business Associate, or its detection but failure to require remediation by Business Associate of an unsatisfactory practice by Business Associate, shall not constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under this Business Associate Agreement or the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.
- 20.6 Section 20.1 is not intended by the parties to limit in any way the scope of Business Associate's obligations related to Inspection and/or Audit and/or similar review in the applicable underlying Agreement, Contract, Participation Agreement, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

21. MISCELLANEOUS PROVISIONS

- 21.1 Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with the terms and conditions of this Business Associate Agreement will be adequate or satisfactory to meet the business needs or legal obligations of Business Associate.
- 21.2 Federal and State Requirements. The Parties agree that the provisions under HIPAA Rules and the California Confidentiality Laws that are required by law to be incorporated into this Business Associate Agreement are hereby incorporated into this Agreement.
- 21.3 No Third-Party Beneficiaries. Nothing in this Business Associate Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
- 21.4 Construction. In the event that a provision of this Business Associate Agreement is contrary to a provision of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, the provision of this Business Associate Agreement shall control. Otherwise, this Business Associate Agreement shall be construed under, and in accordance with, the terms of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without

payment, that gives rise to Contractor's status as a Business Associate.

- 21.5 Regulatory References. A reference in this Business Associate Agreement to a section in the HIPAA Rules means the section as in effect or as amended.
- 21.6 Interpretation. Any ambiguity in this Business Associate Agreement shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA Rules and the California Confidentiality Laws.
- 21.7 Amendment. The parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the HIPAA Rules and any other privacy laws governing Protected Health Information, including the California Confidentiality Laws.

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

AUTHORIZED SIGNORS:

TEHAMA COUNTY

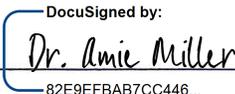
Signed:  Name (Printed): Jayme S. Bottke

Title: Executive Director Date: 3-21-25

Address: P.O. Box 400 Red Bluff, CA 96080

Phone: (530) 528-3216 Email: Jayme.Bottke@tchsa.net

CONTRACTOR: CALIFORNIA MENTAL HEALTH SERVICES AUTHORITY (CalMHSA)

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

Title: Executive Director Date: 4/23/2025

12388-TC-PEERS-25_26
Medi-Cal Peer Support Specialist Certification Program
Tehama County
February 26, 2025

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

Email: amie.miller@calmhsa.org

Exhibit A

DHCS Information Confidentiality And Security Requirements

1. **Definitions.** For purposes of this Exhibit, the following definitions shall apply:
 - a. **Public Information:** Information that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws.
 - b. **Confidential Information:** Information that is exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws.
 - c. **Sensitive Information:** Information that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive Information may be either Public Information or Confidential Information. It is information that requires a higher than normal assurance of accuracy and completeness. Thus, the key factor for Sensitive Information is that of integrity. Typically, Sensitive Information includes records of agency financial transactions and regulatory actions.
 - d. **Personal Information:** Information that identifies or describes an individual, including, but not limited to, their name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It is DHCS' policy to consider all information about individuals private unless such information is determined to be a public record. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request. Personal Information includes the following:

Notice-triggering Personal Information: Specific items of personal information (name plus Social Security number, driver license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person. For purposes of this provision, identity shall include, but not be limited to name, identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph. See Civil Code sections 1798.29 and 1798.82.
2. **Nondisclosure.** Business Associate and its employees, agents, or subcontractors shall protect from unauthorized disclosure any PSCI.
3. Business Associate and its employees, agents, or subcontractors shall not use any PSCI for any purpose other than carrying out the Business Associate's obligations under the JPA Agreement.
4. Business Associate and its employees, agents, or subcontractors shall promptly transmit to Covered Entity's Chief Privacy Officer all requests for disclosure of any PSCI not emanating from the person who is the subject of PSCI.
5. Business Associate shall not disclose, except as otherwise specifically permitted by JPA Agreement or

authorized by the person who is the subject of PSCI, any PSCI to anyone other than DHCS or Covered Entity without prior written authorization from the Covered Entity Chief Privacy Officer, except if disclosure is required by State or Federal law.

6. Business Associate shall observe the following requirements:
 - a. **Safeguards.** Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PSCI, including electronic PSCI that it creates, receives, maintains, uses, or transmits on behalf of Covered Entity. Business Associate shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of Business Associate's operations and the nature and scope of its activities, including at a minimum the following safeguards:
 - i. **Personnel Controls**
 1. **Employee Training.** All workforce members who assist in the performance of functions or activities on behalf of Covered Entity, or access or disclose Covered Entity PSCI, must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.
 2. **Employee Discipline.** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
 3. **Confidentiality Statement.** All persons that will be working with DHCS PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DHCS PHI or PI. The statement must be renewed annually. Business Associate shall retain each person's written confidentiality statement for Covered Entity or DHCS inspection for a period of six (6) years following contract termination.
 4. **Background Check.** Before a member of the workforce may access DHCS PHI or PI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. Business Associate shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

ii. Technical Security Controls

1. **Workstation/Laptop encryption.** All workstations and laptops that process and/or store DHCS PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DHCS Information Security Office.
2. **Server Security.** Servers containing unencrypted DHCS PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
3. **Minimum Necessary.** Only the minimum necessary amount of DHCS PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.
4. **Removable media devices.** All electronic files that contain DHCS PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.
5. **Antivirus software.** All workstations, laptops and other systems that process and/or store DHCS PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.
6. **Patch Management.** All workstations, laptops and other systems that process and/or store DHCS PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.
7. **User IDs and Password Controls.** All users must be issued a unique user name for accessing DHCS PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:
 - Upper case letters (A-Z)

- Lower case letters (a-z)
 - Arabic numerals (0-9)
 - Non-alphanumeric characters (punctuation symbols)
8. **Data Destruction.** When no longer needed, all DHCS PHI or PI must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI or PI cannot be retrieved.
 9. **System Timeout.** The system providing access to DHCS PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
 10. **Warning Banners.** All systems providing access to DHCS PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
 11. **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DHCS PHI or PI, or which alters DHCS PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If DHCS PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.
 12. **Access Controls.** The system providing access to DHCS PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.
 13. **Transmission encryption.** All data transmissions of DHCS PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.
 14. **Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting DHCS PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

iii. Audit Controls

1. **System Security Review.** All systems processing and/or storing DHCS PHI or PI must have at least an annual system risk assessment/security review which

provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

2. **Log Reviews.** All systems processing and/or storing DHCS PHI or PI must have a routine procedure in place to review system logs for unauthorized access.
3. **Change Control.** All systems processing and/or storing DHCS PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

iv. Business Continuity I Disaster Recovery Controls

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

v. Paper Document Controls

1. **Supervision of Data.** DHCS 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.
2. **Escorting Visitors.** Visitors to areas where DHCS PHI or PI is contained shall be escorted and DHCS PHI or PI shall be kept out of sight while visitors are in the area.
3. **Confidential Destruction.** DHCS PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.
4. **Removal of Data.** DHCS PHI or PI must not be removed from the premises of the Business Associate except with express written permission of DHCS.

5. **Faxing.** Faxes containing DHCS PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.
 6. **Mailing.** Mailings of DHCS PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of DHCS PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of DHCS to use another method is obtained.
- b. **Security Officer.** Business Associate shall, to the extent it has not already done so, designate a Security Officer to oversee its data security program who will be responsible for carrying out its privacy and security programs and for communicating on security matters with Covered Entity and DHCS.

Discovery and Notification of Breach. Notice to Covered Entity:

- i. To notify Covered Entity and DHCS **immediately** upon the discovery of a suspected security incident that involves data provided to Covered Entity by DHCS from the Social Security Administration. This notification will be by **telephone call plus email or fax** upon the discovery of the breach. (2) To notify Covered Entity **within 24 hours by email or fax** of the discovery of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of the JPA and this Exhibit, or potential loss of confidential data affecting the JPA. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.
 - ii. Notice shall be provided to the Covered Entity Chief Privacy Officer, the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves data provided to Covered Entity by DHCS from the Social Security Administration, notice shall be provided by calling the DHCS EITS Service Desk. Notice shall be made using the "DHCS Privacy Incident Report" form, including all information known at the time. The Business Associate shall use the most current version of this form, which is posted on the DHCS Privacy Office website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Use" near the middle of the page) or use this link: <http://www.dhcs.ca.gov/formsandoubs/laws/priv/Pacies/DHCSBusinessAssociatesOnl.v.asox>
- c. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI, Business Associate shall take:
- i. Prompt corrective action to mitigate any risks or damages involved with the breach and

to protect the operating environment and

- ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
 - d. **Investigation of Breach.** Business Associate shall immediately investigate such security incident, breach, or unauthorized use or disclosure of PSCI. If the initial report did not include all of the requested information marked with an asterisk, then within seventy-two (72) hours of the discovery, Business Associate shall submit an updated “DHCS Privacy Incident Report” containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Covered Entity Chief Privacy Officer, the DHCS Privacy Officer, and the DHCS Information Security Officer:
 - e. **Written Report.** Business Associate shall provide a written report of the investigation to the Covered Entity Chief Privacy Officer, the DHCS Privacy Officer, and the DHCS Information Security Officer, if all of the required information was not included in the DHCS Privacy Incident Report, within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.
 - f. **Notification of Individuals.** Business Associate shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The Covered Entity Chief Privacy Officer, the DHCS Privacy Officer, and the DHCS Information Security Officer shall approve the time, manner and content of any such notifications.
7. **Effect on lower tier transactions.** The terms of this Exhibit shall apply to all contracts, subcontracts, and subawards, regardless of whether they are for the acquisition of services, goods, or commodities. Business Associate shall incorporate the contents of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.
8. **Contact Information.** To direct communications to the above referenced Covered Entity or DHCS staff, Business Associate shall initiate contact as indicated herein. Covered Entity reserves the right to make changes to the contact information below by giving written notice to Business Associate. Said changes 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
---	-----------------------------	--

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

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

Exhibit B

Privacy and Information Security Provisions

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

Exhibit B consists of the following parts:

1. Exhibit B-1 provides for the privacy and security of PI under Civil Code Section 1798.3(a) and 1798.29.
2. Exhibit B-2, Miscellaneous Provisions, sets forth additional terms and conditions that extend to the provisions of Exhibit B in its entirety.

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

- a. In addition to the Privacy and Security Rules under HIPAA, DHCS is subject to various other legal and contractual requirements with respect to the personal information (as defined in section 2 below) and personally identifiable information (as defined in section 2 below) it maintains. These include:
 - i. The California Information Practices Act of 1977 (California Civil Code §§1798 et seq.),
 - ii. Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2.
- b. The purpose of this Exhibit B-1 is to set forth Business Associate's privacy and security obligations with respect to PI and PII that Business Associate may create, receive, maintain, use, or disclose for or on behalf of Covered Entity pursuant to the JPA Agreement. Specifically this Exhibit applies to PI and PII which is not PHI as defined by HIPAA and therefore is not addressed in this Business Associate Agreement; however, to the extent that data is both PHI or ePHI and PII, both the Business Associate Agreement and this Exhibit B-1 shall apply.
- c. The terms used in this Exhibit B-1, but not otherwise defined, shall have the same meanings as those terms have in the above referenced statute and agreement. Any reference to statutory, regulatory, or contractual language shall be to such language as in effect or as amended.

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

- a. "Breach" shall have the meaning given to such term under the CMPPA (as defined below in Section 2(c)). It shall include a "PII loss" as that term is defined in the CMPPA.
- b. "Breach of the security of the system" shall have the meaning given to such term under the California Information Practices Act, Civil Code section 1798.29(f).
- c. "CMPPA Agreement" means the Computer Matching and Privacy Protection Act ("CMPPA") Agreement between the Social Security Administration and the California Health and Human Services Agency ("CHHS").
- d. "DHCS PI" shall mean Personal Information, as defined below, accessed in a database maintained by the DHCS, received by Business Associate from Covered Entity or acquired or created by Business Associate in connection with performing the functions, activities and services specified in the JPA Agreement on behalf of the Covered Entity.
- e. "Notice-triggering Personal Information" shall mean the personal information identified in Civil Code section 1798.29 whose unauthorized access may trigger notification requirements under Civil Code section 1798.29. For purposes of this provision, identity shall include, but not be limited to,

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

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

3. Terms of Agreement

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

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

b. Responsibilities of Business Associate

Business Associate agrees:

- i. **Nondisclosure.** Not to use or disclose DHCS PI or PII other than as permitted or required by the JPA Agreement or as required by applicable state and federal law.
- ii. **Safeguards.** To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of DHCS PI and PII, to protect against anticipated threats or hazards to the security or integrity of DHCS PI and PII, and to prevent use or disclosure of DHCS PI or PII other than as provided for by the JPA Agreement. Business Associate shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Business Associate's operations and the nature and scope of its activities, which incorporate the requirements of section (c), Security,

below. Business Associate will provide Covered Entity or DHCS with its current policies upon request.

- c. **Security.** Business Associate shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:
- i. Complying with all of the data system security precautions listed in Attachment A, Business Associate Data Security Requirements;
 - ii. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and
 - iii. If the data obtained by Business Associate from DHCS through Covered Entity includes PII, Contractor shall also comply with the substantive privacy and security requirements in the CMPPA Agreement. Business Associate also agrees to ensure that any agents, including a subcontractor to whom it provides DHCS PII, agree to the same requirements for privacy and security safeguards for confidential data that apply to Business Associate with respect to such information.
- d. **Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of DHCS PI or PII by Business Associate or its subcontractors in violation of this Exhibit B-1.
- e. **Business Associate's Agents and Subcontractors.** To impose the same restrictions and conditions set forth in this Exhibit B-1 on any subcontractors or other agents with whom Business Associate subcontracts any activities under the JPA Agreement that involve the disclosure of DHCS PI or PII to the subcontractor.
- f. **Availability of Information to Covered Entity and DHCS.** To make DHCS PI and PII available to Covered Entity or DHCS for purposes of oversight, inspection, amendment, and response to requests for records, injunctions, judgments, and orders for production of DHCS PI and PII. If Business Associate receives DHCS PII, upon request by Covered Entity or DHCS, Business Associate shall provide Covered Entity or DHCS, as applicable, with a list of all employees, contractors and agents who have access to DHCS PII, including employees, contractors and agents of its subcontractors and agents.
- g. **Cooperation with Covered Entity and DHCS.** With respect to DHCS PI, to cooperate with and assist the Covered Entity or DHCS, as applicable, to the extent necessary to ensure DHCS's compliance with the applicable terms of the CIPA including, but not limited to, accounting of disclosures of DHCS PI, correction of errors in DHCS PI, production of DHCS PI, disclosure of a security breach involving DHCS PI and notice of such breach to the affected individual(s).
- h. **Confidentiality of Alcohol and Drug Abuse Patient Records.** Business Associate agrees to comply

with all confidentiality requirements set forth in Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2. Business Associate is aware that criminal penalties may be imposed for a violation of these confidentiality requirements.

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

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

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

1. **Disclaimer.** Covered Entity makes no warranty or representation that compliance by Business Associate with this Exhibit B, HIPAA or the HIPAA regulations will be adequately or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of the DHCS PHI, PI and PII.
2. **Amendment.** The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Exhibit B may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations, and other applicable state and federal laws. Upon either party's request, the other party agrees to promptly enter into negotiations concerning an amendment to this Exhibit B embodying written assurances consistent with requirements of HIPAA, the HITECH Act, and the HIPAA regulations, and other applicable state and federal laws. Covered Entity may terminate the JPA Agreement upon thirty (30) days written notice in the event:
 - a. Business Associate does not promptly enter into this Exhibit B when requested by Covered Entity; or
 - b. Business Associate does not enter into an amendment providing assurances regarding the safeguarding of DHCS PHI that the DHCS deems is necessary to satisfy the standards and requirements of HIPAA and the HIPAA regulations
3. **Judicial or Administrative Proceedings.** Business Associate will notify Covered Entity and DHCS if it is named as a defendant in a criminal proceeding for a violation of HIPAA or other security or privacy law. Covered Entity may at the request of DHCS terminate the JPA Agreement if Business Associate is found guilty of a criminal violation of HIPAA. Covered Entity may at the request of DHCS terminate the JPA Agreement if a finding or stipulation that Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined. DHCS will consider the nature and seriousness of the violation in deciding whether or not to request that Covered Entity terminate the JPA Agreement.
4. **Assistance in Litigation or Administrative Proceedings.** Business Associate shall make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under the JPA Agreement, available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers or employees based upon claimed violation of HIPAA, or the HIPAA regulations, which involves inactions or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named adverse party.
5. **No Third-Party Beneficiaries.** Nothing express or implied in the terms

and conditions of this Exhibit B is intended to confer, nor shall anything herein confer, upon any person other than the Covered Entity or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

6. **Interpretation.** The terms and conditions in this Exhibit B shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, and the HIPAA regulations. The parties agree that any ambiguity in the terms and conditions of this Exhibit B shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations, and, if applicable, any other relevant state and federal laws.
7. **Conflict.** In case of a conflict between any applicable privacy or security rules, laws, regulations or standards the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI, PI and PII from unauthorized disclosure. Further, Business Associate must comply within a reasonable period of time with changes to these standards that occur after the effective date of the JPA Agreement.
8. **Regulatory References.** A reference in the terms and conditions of this Exhibit B to a section in the HIPAA regulations means the section as in effect or as amended.
9. **Survival.** The respective rights and obligations of Business Associate under Item 3(b) of Exhibit B-1, Responsibilities of Business Associate, shall survive the termination or expiration of this Agreement.
10. **No Waiver of Obligations.** No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.
11. **Audits, Inspection and Enforcement.** From time to time, and subject to all applicable federal and state privacy and security laws and regulations, Covered Entity or DHCS may conduct a reasonable inspection of the facilities, systems, books and records of to monitor compliance with this Exhibit B. Business Associate shall promptly remedy any violation of any provision of this Exhibit B. The fact that Covered Entity or DHCS inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Exhibit B. Covered Entity's or DHCS's failure to detect a non-compliant practice, or a failure to report a detected noncompliant practice to Business Associate does not constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under the JPA Agreement or related documents, including this Exhibit B.
12. **Due Diligence.** Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Exhibit B and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and other applicable state and federal law, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Exhibit B.
13. **Term.** The Term of this Exhibit B shall extend beyond the termination of the Agreement and shall terminate when all DHCS PHI is destroyed or returned to Covered Entity, in accordance with 45 CFR Section 1 64.504(e)(2)(ii)(1), and when all DHCS PI and PII is destroyed in accordance with Attachment

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

Attachment A to Exhibit B-2
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 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:
 - i. Upper case letters (A-Z)
 - ii. Lower case letters (a-z)
 - iii. Arabic numerals (0-9)
 - iv. Non-alphanumeric characters (punctuation symbols)
- h. **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.
- i. **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.
- j. **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.

- k. **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.
- l. **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.
- m. **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.
- n. **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 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.



State of California—Health and Human Services Agency
Department of Health Care Services



GAVIN NEWSOM
GOVERNOR

DATE: July 22, 2021

Behavioral Health Information Notice No: 21-041

TO: California Alliance of Child and Family Services
California Association for Alcohol/Drug Educators
California Association of Alcohol & Drug Program Executives, Inc.
California Association of DUI Treatment Programs
California Association of Mental Health Peer Run Organizations
California Association of Social Rehabilitation Agencies
California Behavioral Health Planning Council
California Consortium of Addiction Programs and Professionals
California Council of Community Behavioral Health Agencies
California Opioid Maintenance Providers
California State Association of Counties
Coalition of Alcohol and Drug Associations
County Behavioral Health Directors
County Behavioral Health Directors Association of California
County Drug & Alcohol Administrators
United Parents

SUBJECT: Medi-Cal Peer Support Specialist Certification Program
Implementation

PURPOSE: To provide the standards for implementing the Medi-Cal Peer Support
Specialist Certification Program.

REFERENCE: Centers for Medicare and Medicaid Services State Medicaid Directors
Letter #07-011
Welfare and Institutions Code, Division 9, Part 3, Article 1.4, Chapter 7

BACKGROUND:

DHCS acknowledges the role that peer support specialists (hereafter referred to as “peers”) can play in California’s behavioral health systems, and recognizes that peers have long acted as a part of the prevention, early intervention, treatment, and recovery process for individuals living with Mental Health (MH) conditions and Substance Use Disorders (SUD)s. As individuals with either lived experience, or as the parents, caregivers and family members of individuals living with MH and/or SUD conditions,

Behavioral Health Information Notice No.: 21-041
Page 2
July 22, 2021

peers personally understand the experience of the individuals they serve and can help clarify the most effective set of services for each individual's recovery needs.

Senate Bill (SB) 803, chaptered in 2020, authorized DHCS to seek federal approvals to add peer support specialists as a Medi-Cal provider type and peer support services as a distinct service type in counties opting to participate in this program. DHCS is pursuing these federal approvals through the Medicaid waiver and State Plan Amendment processes.

SB 803 also directed DHCS to develop state standards for Medi-Cal Peer Support Specialist Certification Programs that may be implemented by counties, or county-contracted entities, who opt in to provide these programs. This certification is required for Medi-Cal reimbursement, but does not impact peer programs under other funding sources. DHCS has worked extensively with stakeholders to develop these state standards, including multiple behavioral health and peer-led associations, county partners, representatives from various non-profit organizations, representatives from peer-run organizations, existing peer support specialists, consumers, and other interested individuals.

This BHIN provides state standards for California's Medi-Cal Peer Support Specialist Certification Programs and the steps counties who opt in must take to implement these programs. Future guidance will be provided on the implementation of the Peer Support Services Medi-Cal benefit.

POLICY:

SB 803 created the statutory authority for DHCS to establish Medi-Cal statewide certification program standards while counties, or county-contracted entities, are responsible for implementing the programs at the local level. (W&I Code Section 14045.14) By July 1, 2022, DHCS must:

1. Establish statewide requirements to use in developing certification programs
2. Define the qualifications, range of responsibilities, practice guidelines, and supervision standards for peer support specialists
3. Determine the process for initial certification
4. Determine curriculum and core competencies required for certification, including areas of specialization
5. Specify peer support specialist employment training requirements
6. Establish a code of ethics
7. Determine a biennial certification renewal process, including continuing education requirements
8. Determine a process for investigation of complaints and corrective action

Behavioral Health Information Notice No.: 21-041
Page 3
July 22, 2021

9. Determine a process for an individual employed as a peer support specialist on January 1, 2022, to obtain certification
10. Determine requirements for peer support specialist certification reciprocity between counties and out of state

California Medi-Cal Peer Support Specialist Certification Program Standards

Medi-Cal Peer Support Specialist Certification Programs can be established either by counties, or an agency representing counties. The County Behavioral Health Directors' Association (CBHDA) has identified the California Mental Health Services Authority (CalMHSA) as the entity that will represent counties for the implementation of a State-approved Medi-Cal Peer Support Specialist Certification Program, to support consistency statewide.

CalMHSA, on behalf of the counties they represent, and any other counties that seek to implement their own Medi-Cal Peer Support Specialist Certification Program, must adhere to the standards set forth in Enclosure 1 of this BHIN and must submit to DHCS their application with supporting documents that will be used to implement their program in accordance with Enclosure 2.

Each Medi-Cal Peer Support Specialist Certification Program must ensure that certified peers meet the following qualifications:

1. Be at least 18 years of age.
2. Possess a high school diploma or equivalent degree.
3. Be self-identified as having experience with the process of recovery from mental illness or substance use disorder, either as a consumer of these services or as the parent, caregiver or family member of a consumer.
4. Be willing to share their experience.
5. Have a strong dedication to recovery.
6. Agree, in writing, to adhere to a code of ethics.
7. Successfully complete the curriculum and training requirements for a peer support specialist.
8. Pass a certification examination approved by DHCS for a peer support specialist.

Counties, or an agency representing a county, pursuing the development of a Medi-Cal Peer Support Specialist Certification Program will be subject to periodic reviews conducted by DHCS to ensure adherence to all federal and state requirements, and must submit annual peer support specialist program reports to the department.

Application and Submission Requirements

DHCS encourages counties to take advantage of the opportunity to work with CalMHSA for their certification programs. Any county not working with CalMHSA must notify

Behavioral Health Information Notice No.: 21-041
Page 4
July 22, 2021

DHCS by August 6, 2021. Counties can send this information to DHCS via email at Peers@dhcs.ca.gov.

CalMHSA, on behalf of counties they represent, and any other counties developing their own certification programs must apply to DHCS by submitting the documents listed in Enclosure 2, and receive approval, prior to implementing a certification program. The program plan shall include: proposed policies and procedures for a candidate's initial certification, including the training curriculum for peers and peer supervisors; the certification exam; the process for biennial and lapsed renewals; the curriculum for the identified areas of specialization; the grandparenting process for qualifying peers; the complaints and corrective actions process; and a certification fee schedule.

Medi-Cal Peer Support Specialist Certification Program plans must be in an electronic format and sent to Peers@dhcs.ca.gov. The opportunity for counties to implement a certification program will be made available annually. For FY 2021-22, counties must submit the certification plan documents prior to November 19, 2021.

List of Enclosures

1. Standards for Initial Certification, Biennial Renewal, Lapsed Certification, Areas of Specialization, Grandparenting, State/County Reciprocity, Complaints and Corrective Actions
2. Medi-Cal Peer Support Specialist Certification Program Plan Submission Requirements
3. Medi-Cal Code of Ethics for Peer Support Specialists in California
4. Practice Guidelines and Supervision Standards
5. Reporting Requirements

Sincerely,

Marlies Perez, Division Chief
Community Services Division

Behavioral Health Information Notice No.: 21-041
Page 5
July 22, 2021

ENCLOSURE 1

1. Initial Certification
2. Biennial Renewal
3. Lapsed Certification
4. Areas of Specialization,
5. Grandparenting, State/County Reciprocity
6. Complaints and Corrective Actions

1. *Standards for Initial Certification of a Peer Support Specialist*

For an initial certification of a peer support specialist, a Medi-Cal Peer Support Specialist Certification Program must:

- A. Ensure a candidate agrees to adhere to the Medi-Cal Code of Ethics for Peer Support Specialists
- B. Ensure a candidate has completed the training curriculum that includes 80 hours of training - including didactic learning
- C. Ensure the candidate has passed the initial certification exam

A. Medi-Cal Code of Ethics

The Medi-Cal Code of Ethics for Peer Support Specialists is contained in Enclosure 3 and posted on the DHCS Peers webpage. DHCS will update the Code of Ethics as appropriate and certification programs must ensure that candidates agree to adhere to the most recent version posted.

B. Training Curriculum

The training curriculum must incorporate the following core competencies:

1. The concepts of hope, recovery, and wellness.
2. The role of advocacy.
3. The role of consumers and family members.
4. Psychiatric rehabilitation skills and service delivery, and addiction recovery principles, including defined practices.
5. Cultural and structural competence trainings.
6. Trauma-informed care.
7. Group facilitation skills.
8. Self-awareness and self-care.
9. Co-occurring disorders of mental health and substance use.
10. Conflict resolution.
11. Professional boundaries and ethics.
12. Preparation for employment opportunities, including study and test-taking skills, application and résumé preparation, interviewing, and other potential requirements for employment.

Behavioral Health Information Notice No.: 21-041
Page 6
July 22, 2021

13. Safety and crisis planning.
14. Navigation of, and referral to, other services.
15. Documentation skills and standards.
16. Confidentiality.
17. Digital literacy.

C. Certification Exam

Upon a candidate's completion of the training, a Medi-Cal Peer Support Specialist Certification Program must administer an examination that has been approved by DHCS. The Medi-Cal Peer Support Specialist Certification Program must provide reasonable accommodations to candidates taking the examination, as needed, including verbal testing and testing in prevalent languages.

2. *Standards for Biennial Renewal*

A Medi-Cal Peer Support Specialist Certification Program must provide a process for biennial certification renewal for certified peer support specialists. This process must include making available continued education trainings and ensuring that renewal candidates perform 20 hours of continuing education every two years. The continuing education must include updates on applicable laws and evidence based best practices. A Medi-Cal Peer Support Specialist Certification Program must also ensure that certified peer support specialists reaffirm in writing the most recent version of the Medi-Cal Code of Ethics for Peer Support Specialists in California every two years.

3. *Lapsed Certification*

For peer support specialists whose certification lapsed, but is still within four years of when certification renewal was due, a Medi-Cal Peer Support Specialist Certification Program must allow certification if the candidate completes 40 hours of refresher training¹, passes the Medi-Cal Peer Support Specialist Certification Program examination, and must affirm, in writing, the most recent version of the Medi-Cal Code of Ethics for Peer Support Specialists in California.

4. *Areas of Specialization*

A Medi-Cal Peer Support Specialist Certification Program must implement a curriculum in the area of specialization for "Parent, Caregiver, and Family Member Peers" upon implementation of the Peer Support Specialist Certification Program.

The following three areas of specialization must also be implemented by January 1, 2023:

- Crisis Services

¹ This training must still cover the core competencies, but would be a condensed version of the full 80 hour curriculum. This refresher curriculum must also be approved by DHCS.

Behavioral Health Information Notice No.: 21-041
Page 7
July 22, 2021

- Forensic (Justice Involved)
- Homelessness

These areas of specialization must be developed in addition to the requirements for certification in the core competencies, and the curriculums must be approved by DHCS.

DHCS will continue to collect information on areas of specialization that may be added at a later date. Any additional areas of specialization must be approved by DHCS.

5. Grandparenting and Out-of-State Reciprocity

For individuals who are employed as a peer as of January 1, 2022 and seek certification under these standards, known in this BHIN as grandparenting, or those individuals certified out of state and are seeking to be certified under these standards, a Medi-Cal Peer Support Specialist Certification Program must grant certification if the individual has:

Either:

- 1 year of paid or unpaid work experience (1550 hours) as a peer specialist AND 20 hours of continuing education (CEs), including law and ethics. CEs can be in relevant professional competencies obtained via relevant in-state, out of state or national educational forums.

OR

- 1550 hours in 3 years, with 500 hours completed within the last 12 months, working as a peer specialist AND 20 hours of continuing education (CEs), including law and ethics. CEs can be in relevant professional competencies obtained via relevant in-state, out of state or national educational forums.

AND has all of the following:

- Completion of a peer training(s)
- 3 Letters of Recommendation as outlined:
 - One from a supervisor
 - One from a colleague/professional
 - One self-recommendation describing their current role and responsibilities as a peer support specialist
- Pass the Medi-Cal Peer Support Specialist Certification Program Exam

Behavioral Health Information Notice No.: 21-041
Page 8
July 22, 2021

As with the initial certification, the Medi-Cal Peer Support Specialist Certification Program must provide reasonable accommodations to the candidate as requested, including verbal testing and testing in prevalent languages.

Peers employed as a peer January 1, 2022 and seeking certification through the grandparenting process must complete or begin the process by December 31, 2022. After this date, peers seeking certification under a Medi-Cal Peer Support Specialist Certification Program must complete the initial certification process. Peers with out of state certification seeking reciprocity have no sunset date to seek certification.

6. County Reciprocity

Peer Support Specialists who are certified through a DHCS approved Medi-Cal Peer Support Specialist Certification Program will be recognized as a Certified Peer Support Specialist in all counties throughout California however, only counties electing to participate in the Medi-Cal peers benefit will have the ability to be federally reimbursed for behavioral health peer services provided to Medi-Cal beneficiaries.

7. Complaints and Corrective Actions

A Medi-Cal Peer Support Specialist Certification Program must also submit a process for reviewing complaints and corrective actions, including the suspension and revocation of certification, as well as the appeals process for DHCS approval. DHCS will approve processes that include the following:

- Specifications for the Medi-Cal Peer Support Specialist Certification Program to investigate submitted complaints within a specified timeframe.
- A disciplinary process for substantiated allegations that requires either education hours, suspension, and/or revocation.
- An appeal process.

Monitoring of the program will be incorporated into DHCS' current processes, including DHCS' triennial audits and the EQRO quality improvement program efforts.

Behavioral Health Information Notice No.: 21-041
 Page 9
 July 22, 2021

ENCLOSURE 2 – Medi-Cal Peer Support Specialist Certification Program Plan Submission requirements

Submission Package for Medi-Cal Peer Support Specialist Certification Program		
<p>CalMHSA, on behalf of represented counties, and other counties who seek to implement a Medi-Cal Peer Support Specialist Certification Program must submit a plan for DHCS approval of how the certification program will meet all of the federal and state requirements for the certification and oversight of peer support specialists (W&I Code 14045.14 (a)(1)).</p> <p>Please include the signature of the authorized representative from CalMHSA, or the county Behavioral Health Director.</p> <p>The plan must include the following:</p>		
<input type="checkbox"/>	Initial Certification Policies And Procedures	How applicants can apply for certification and how the training curriculum and the exam will be administered.
<input type="checkbox"/>	Certification Exam	The exam that applicants will be required to take. Also include the alternative ways the exam will be administered for those with difficulty taking written exams. Include accommodations that will be available for those with disabilities, or those who require translations or interpreters, including the prevalent languages in which the exam will be made available.
<input type="checkbox"/>	Biennial Certification Renewal Policies And Procedures	How the program will make continuing education (CE) training available for certified peers, how certified peers can demonstrate successful completion of CE training, and how peers can submit a renewal of the Code of Ethics.
<input type="checkbox"/>	Training Curriculum For: <ul style="list-style-type: none"> • Peer Support Specialist • Parent, Caregiver and Family Member Peers • Peer Supervisors 	The curriculum for initial certification, the curriculum for lapsed certification, a curriculum for the area of specialization for parent, caregiver and family member peers, and peer supervisors.
<input type="checkbox"/>	Certification Fee Schedule	Per W&I Code Section 14045.18, a participating county, or an agency representing a participating county, is authorized to establish a certification fee schedule for the purpose of supporting the activities associated with the ongoing administration of the peer support specialist certification program. Before the fee schedule may be implemented, the department shall review and either approve or disapprove the fee schedule of the participating county or an agency representing the participating county.

Behavioral Health Information Notice No.: 21-041

Page 10

July 22, 2021

<input type="checkbox"/>	Grandparenting/Reciprocity Process	The policies and procedures for how an applicant can apply for certification and how the program will operationalize reviewing applications and issuing the certification.
<input type="checkbox"/>	Complaints/Corrective Actions Process	The policies and procedures for how complaints will be submitted and processed, including a timeline, disciplinary actions, and appeals process.
<input type="checkbox"/>	Reporting Process	The policies and procedures for the timely submission of the identified data to meet the reporting requirements.

ENCLOSURE 3 – Medi-Cal Code of Ethics for Peer Support Specialists in California

Purpose	<p>Peer support services are recovery-oriented and resiliency-focused services for those managing behavioral health challenges as well as the parents, family members, and caregivers that support them. Peer support services are evidence-based practices that provide role models to inspire hope, demonstrate a life of recovery and resiliency, and encourage real advocacy.</p> <p>This Values and Ethics document promotes a consistent message to those who are providing, receiving, and supervising services from a Peer Support Specialist. The Values and Ethics described here formalizes and advances peer support services in California’s behavioral health system of care.</p> <p>For the purpose of this document “Peer Support Specialist” refers to anyone who is providing services in the behavioral health field using their “lived experience” to establish mutuality and build resiliency and recovery.</p>
Values Hope	<p>Ethical Standards</p> <p>Peer Support Specialists:</p> <ul style="list-style-type: none"> • Inspire hope in those engaging in services by living a life of Recovery and/or Resiliency.
Person-Driven	<p>Peer Support Specialists:</p> <ul style="list-style-type: none"> • Support individuals receiving services and their support network within the context of the individual’s worldview, to achieve their goals based upon their needs and wants. • Focus on self-determination, as defined by the person engaging in services, and support the person’s participation in their own recovery. • Inform others about options, provide information about choices, and then respect peers’ decisions. • Encourage people to look at the options, take risks, learn from mistakes, and grow toward healthy interdependence with others. • Uphold the principle of non-coercion as essential to recovery and encourage those engaging in services to make their own decisions, even when the person engaging in services is under mandated treatment. • Assist those they support to access additional resources. • Disclose lived experiences of recovery in a way that maintains the focus on and is beneficial to the person engaging in services. • Support the recovery process for the peer, allowing the person to direct their own process.

**Family Driven
and Child-
Centered**

- Shall not force any values or beliefs onto the person engaging in services.
 - Recognize there are many pathways to recovery that can be very different than their own journey.
- Peer Support Specialists:
- Promote the family member's ethical decision-making and personal responsibility consistent with that family member's culture, values, and beliefs.
 - Respect and value the beliefs, opinions, and preferences of children, youth, family members, parents, and caregivers in service planning.
 - Promote the family members' voices and the articulation of their values in planning and evaluating behavioral health related challenges or concerns.
 - Support other family members as peers with a common background and history.
 - Disclose personal lived experiences of building resiliency in a way that focuses on and is beneficial to the child, youth, family member, parent, or caregiver engaging in services.
 - Build supports on the strengths of the child, youth, family, or caregiver.
 - Build partnerships with others who are involved in the care of our children, youth, or adult family members.
 - Communicate clearly and honestly with children, youth, family members, and caregivers.

**Holistic
Wellness**

- Peer Support Specialists:
- Promote the family member's ethical decision-making and personal responsibility consistent with that family member's culture, values, and beliefs.
 - Practice in a holistic manner that considers and addresses the whole health of those engaging in services.
 - Recognize the impact of co-occurring challenges (substance use, developmental and physical challenges) in the recovery resiliency journey and provide supports sensitive to those needs.
 - Recognize the impact of trauma on the recovery/resiliency journey and provide the support specific to those challenges.
 - Honor the right of persons engaging in services to choose alternative treatments and practices, including culturally-specific traditional methods, healing arts, including acupuncture and meditation, spiritual practices or secular beliefs, and harm reduction practices.

Authenticity

- Peer Support Specialists:
- Practice honest and direct communication in a culturally relevant manner, saying what is on their mind in a respectful way. Difficult circumstances are addressed with those who are directly involved. Direct communication

**Cultural
Responsiveness
& Humility**

moves beyond the fear of conflict or hurting other people to the ability to work together to resolve challenges with caring and ~~compassion~~

- Share own lived experience to provide hope and inspiration for recovery.
- Practice healthy disclosure about their own experience focused on providing hope and direction toward recovery and/or resiliency.
- Work within their scope of practice as defined by this Code of Ethics and their employing agency.
- Remain aware of their skills and limitations, and do not provide services or represent themselves as an expert in areas for which they do not have sufficient knowledge or expertise.
- Know that maintaining the authenticity and integrity of their role is critical to the effectiveness of peer support services.
- Seek supervision, peer support services, and/or other contact with peer colleagues or other supports to stay within their scope of practice.

Peer Support Specialists:

- Acknowledge the importance of language and culture, intersecting identities, knowledge, and acceptance of dynamics of cultural differences, expansion of cultural knowledge, curiosity, and adaptation of services to meet culturally unique needs.
- Strive to provide culturally responsive and relevant services to those they support.
- Respect cultural identities and preferences of those engaging in services and their families and respect the right of others to hold opinions, beliefs, and values different from their own.
- Shall not discriminate against others on the basis of gender, race, ethnicity, sexual orientation or gender identity, ~~age~~ religion, national origin, marital status, political belief, or mental or physical differences.
- Shall not discriminate against others on the basis of any other preference, personal characteristic, condition, state, or cultural factor protected under Federal, State or local law.
- Seek further information, education, and training in cultural competence as necessary to assist those they support.

Respect

Peer Support Specialists:

- Provide a welcoming environment for persons engaging in services.
- Approach each person, youth, parent or family member with openness, genuine interest, and appreciation.
- Accept each person/family and situation as unique.
- Provide empathy and able to “put oneself in the other person’s shoes.”
- Will make an honest effort to empathize with the emotional connection and cultural context that the persons engaging in services bring to the

recovery/ resiliency relationship.

- View everyone as having something important and unique to contribute.
- Value and treat others with kindness, warmth, dignity, and without judgment.
- Accept each other and are open to sharing with people from many diverse backgrounds including ethnicity, educational levels, socio-economic background, sexual preference, and religion/spirituality.
- Honor and make room for everyone's opinions and see each other as equally capable of contributing.
- Demonstrate respect toward those supported, colleagues and the community.
- Use language that is respectful, "person-first," and culturally mindful to, and with, those supported, colleagues and the community.
- Never use language that could be construed as, or is, derogatory, insulting, or demeaning in written, electronic, or verbal communications.
- Communicate with co-workers and colleagues in ways that promote hope, compassion, and solution-focused interactions.

Integrity

Peer Support Specialists:

- Act in accordance with the highest standards of professional integrity.
- Avoid relationships or commitments that conflict with the interests of persons engaging in services, impair professional judgment, imply a conflict of interest, or create risk of harm to those supported.
- Conduct themselves in a way that does not jeopardize the integrity of the peer relationship.
- Seek supervision to handle any real or potential conflicts when and if a dual relationship is unavoidable.
- Follow organizational policies and guidelines regarding giving and receiving gifts.
- Consider the cultural context and other potential considerations related to gifts.
- Do not lend, give, or receive money or payment for any services to, or from, persons they support.
- Demonstrate accountability in fulfilling commitments.
- Resist influences that interfere with professional performance.
- Shall not commit fraud, waste or abuse in the delivery of Medi-Cal services.
- Cooperate with complaint investigations and supply information requested during complaint investigations unless such disclosure of information would violate the confidentiality requirements of Subpart 2, Title 42, Code of Federal Regulations.

Behavioral Health Information Notice No.: 21-041
Page 15
July 22, 2021

- Shall not provide services under the influence of any amount of alcohol, marijuana, or illicit drugs. “Illicit drugs” means any substance defined as a drug in Section 11014, Chapter 1, Division 10, Health and Safety Code, except:
 - Drugs or medications prescribed by a physician or other person authorized to prescribe drugs, in accordance with Section 4036, Chapter 9, Division 2, Business and Professions Code, and used in the dosage and frequency prescribed; or
 - Over-the-counter drugs or medications used in the dosage and frequency described on the box, bottle, or package insert.
- Shall not secure a certification by fraud, deceit, or misrepresentation. This includes, but is not limited to:
 - Making a false statement on any application for certification.
 - Withholding material information on any application for certification.
 - Impersonating another Peer Support Specialist or permitting or allowing another person to use their certification for the purpose of providing peer support services.
- Shall not engage in gross negligence or incompetence in the performance of peer support services. This includes:
- Failing to maintain records consistent with sound judgement, the standards of the profession, and the nature of the services being rendered.

Advocacy

Peer Support Specialists:

- Support the formulation, development, enactment, and implementation of public policies of concern to the profession.
- Demonstrate and promote activities that respect diversity.
- Support and defend human rights and freedoms regardless of nationality, national origin, gender identity, ethnicity, religion or spiritual persuasion, language, disability, sexual identity, or socio-economic status. Human rights include civil and political rights, such as the right to life, liberty, and freedom of expression; social, cultural, and economic rights including the right to cultural expression, the right to have basic needs met, and the right to work and receive an education.
- Advocate for inclusion of those supported in all aspects of services.
- Advocate for the full involvement of those supported in the communities of their choice and will promote their value to those communities.
- Understand, encourage, and empower self-advocacy.
- Recognize that all individuals/families have the right to live in the safest and least restrictive, culturally congruent environment.
- Strive to eliminate stigma and discrimination

Confidentiality

Peer Support Specialists:

- Respect the rights, dignity, privacy, and confidentiality of persons engaging in services at all times.
- Respect the right to privacy of those supported and shall not solicit private information from those supported unless it is essential. Once private information is shared, standards of confidentiality apply.
- Respect confidential information shared by colleagues in the course of their professional relationships and interactions unless such information relates to an unethical or illegal activity. However, confidentiality should be honored when Peers are supporting clients with a substance use disorder where the illegal activity is limited to personal use of substances.
- Comply with all applicable federal and state confidentiality laws and guidelines. (In accordance with Part 2, Title 42, Code of Federal Regulations and HIPAA requirements).
- Discuss with persons engaging in services, and other interested parties, the nature of confidentiality and limitations of the right to confidentiality.

Safety & Protection

Peer Support Specialists:

- Never engage in romantic or sexual/intimate activities with the persons engaging in services.
- Shall not provide services to individuals with whom they have had a prior romantic or sexual relationship.
- Shall not engage in exploitive relationships with coworkers or those they support to further their personal, religious, political, or business interests.
- Follow applicable federal, state and local laws in the prevention of harm.
- Inform appropriate persons when disclosure is necessary to prevent serious, foreseeable, and imminent harm to persons served or other identifiable persons. In all instances, Peer Support Specialists should disclose the least amount of confidential information necessary to achieve the desired purpose.
- Never intimidate, threaten, harass, use undue influence, physical force, or verbal abuse, or make unwarranted promises of benefits to persons engaging in services.
- Recognize the unique nature of the peer relationship and seek supervision and/or peer support services, as necessary, to maintain appropriate boundaries with persons engaging in services.
- Treat colleagues with respect, courtesy, fairness, and good faith, and uphold the Code of Ethics.
Strive to provide a safe environment that is respectful of the impact of trauma on persons engaging in services.

Education

Peer Support Specialists:

Mutuality	<ul style="list-style-type: none">• Remain current regarding new developments in recovery, resiliency and wellness theories, methods, and approaches of related disciplines/systems with whom those who are engaging in services interface.• Accept responsibility for continuing education and professional development as part of their commitment to provide quality services.• Become familiar with local resources for self-sufficiency, including benefits and employment opportunities and supportive resources for families, parents, and caregivers. <p>Peer Support Specialists:</p> <ul style="list-style-type: none">• Engage in a relationship of mutual responsibility where power is shared and the Peer Support Specialist and the persons engaging in services are equally responsible for maintaining a peer relationship that is mutually beneficial.• Take responsibility for voicing their own needs and feelings.• Make decisions in collaboration with persons served and do not make decisions for persons engaging in services.• Ensure that people give and take the lead in discussions, everyone is offered a chance to speak, and decisions are made in collaboration with one another.
Reciprocity	<p>Peer Support Specialists:</p> <ul style="list-style-type: none">• Ensure that the relationship is reciprocal. Every participant in the peer relationship both gives and receives in a fluid, constantly changing dynamic.• Belief that peer relationships are not hierarchical; no one is more qualified, advanced, or better than another.• Learn from each other.• View asking for help as reaching across (not up nor down).
Strengths-Based	<p>Peer Support Specialists:</p> <ul style="list-style-type: none">• Provide strength-based services acknowledging that every person has skills, gifts, and talents they can use to better their lives.• Focus on what is strong, not what is wrong.• Assist others to identify these strengths and explore how those identified strengths can be used for their benefit.
Wellness, Recovery and Resiliency	<p>Peer Support Specialists:</p> <ul style="list-style-type: none">• Engage in and model regular self-care activities.• Communicate and behave in ways that promote wellness, recovery, and resiliency.• Use language that reflects wellness, recovery, and resiliency principles.• Shall not impose limitations on the possibility for wellness, recovery, and

Behavioral Health Information Notice No.: 21-041
Page 18
July 22, 2021

- resiliency of those engaging in services.
- Recognize the importance of supportive relationships and community in wellness, recovery and resiliency and encourage persons to identify and develop natural supports.
- Promote self-sufficiency in the wellness, recovery, and resiliency journey.

Wellness is the conscious and deliberate process of creating and adapting patterns of behavior that lead to improved health in the following wellness dimensions: Emotional, Financial, Social, Spiritual, Educational/Occupational, Physical, Intellectual, and Environmental.

Recovery is a process of change through which individuals improve their health and wellness, live a self-directed life, and strive to reach their full potential. This process of change recognizes cultural diversity and inclusion and honors the different routes to resilience and recovery based on the individual and their cultural community.

Resiliency is an inner capacity that, when nurtured, facilitated, and supported, empowers individuals and communities to successfully meet life's challenges with a sense of self-determination, mastery and hope.

By signing below, I agree not to violate, or assist in or abet the violation of, or conspire to violate, any provision or term of this Code of Ethics. All Peer Support Specialists shall be notified, in writing, of any changes to this Code of Ethics.

Name (printed)

Name (signature)
Date (mm/dd/yyyy)

Behavioral Health Information Notice No.: 21-041
Page 19
July 22, 2021

Enclosure 4 – Practice Guidelines and Supervision Standards

Practice Guidelines

Counties must use the practice guidelines developed by the Substance Abuse and Mental Health Services Administration, *What are Peer Recovery Support Services*.

Supervision Standards

DHCS acknowledges the efficacy and evidenced based practice of the utilization of certified peer support specialists as supervisors of other peers. DHCS highly encourages the employment of peers as peer supervisors. However, due to the variability of counties and availability of the peer workforce, DHCS will allow the utilization of other behavioral health professionals as follows:

Peer Support Specialist Supervisors must meet at least one of the below qualifications:

- Have a Medi-Cal Peer Support Specialist Certification Program certification; have two years of experience working in the behavioral health system; and have completed a DHCS approved peer support supervisory training curriculum.
OR
- Be a non-peer behavioral health professional (including registered & certified SUD counselors) who has worked in the behavioral health system for a minimum of two years, and has completed a DHCS approved peer support supervisory training;
OR
- Have a high school diploma or GED, four years of behavioral health direct service experience that may include peer support services; and have completed an approved peer support supervisory training curriculum.

Behavioral Health Information Notice No.: 21-041
 Page 20
 July 22, 2021

ENCLOSURE 5 – Annual Reporting Requirements

California Peer Support Specialist Certification Program Annual Reporting Requirements		
<p>Reports must reflect information on certifications occurring within a fiscal year (July 1 – June 30), and are due to DHCS by the December 31st following the end of the fiscal year. DHCS may add additional reporting requirements in subsequent years. Reports must contain the following information:</p>		
1) Number Of Peer Support Specialists Certified:		[field]
2) Number Of Applicants That Did Not Receive Certification:		[field]
3) Number Of Applicants Employed In Peer Services Prior To Certification:		[field]
4) Number Of Applicants Certified In An Area Of Specialization:		
	a) Crisis Services	[field]
	b) Homeless	[field]
	c) Forensic	[field]
	d) Parent, Caregiver and Family Member Peer	[field]
5) Number Of Certified Peers That Renewed Certification:		[field]
6) Number Of Peer Supervisor Trainings Provided:		[field]
7) (For FY 2021-2022) Number of Applicants that received Certification through Grandparenting Process:		[field]
8) Number of Applicants that received Certification through State Reciprocity:		[field]
9) Peer Support Specialist Demographics		
	a) Age	
	i. 18-25	[field]
	ii. 26-64	[field]

Behavioral Health Information Notice No.: 21-041
 Page 21
 July 22, 2021

	iii. 65+	[field]
	b) Gender Identity	
	i. Male	[field]
	ii. Female	[field]
	iii. Non-binary	[field]
	c) Race/Ethnicity	
	i. American Indian/Alaskan Native	[field]
	ii. Asian/Pacific Islander	[field]
	iii. Black	[field]
	iv. Hispanic	[field]
	v. White	[field]
	vi. Not Reported	[field]
	d) Proficient Languages (multi-lingual peers may be counted under multiple fields)	
	i. Arabic	[field]
	ii. Armenian	[field]
	iii. Cambodian	[field]
	iv. Chinese (combined Cantonese or Mandarin)	[field]
	v. English	[field]
	vi. Farsi	[field]
	vii. Hmong	[field]
	viii. Korean	[field]
	ix. Russian	[field]

Behavioral Health Information Notice No.: 21-041
Page 22
July 22, 2021

	x. Spanish	[field]
	xi. Tagalog	[field]
	xii. Vietnamese	[field]

E-Contract Review
Approval as to Form

Department Name: Health Services Agency

Vendor Name: CalMHSA

Contract Description: For the purpose of Medi-Cal Peer support participation

APPROVED AS TO FORM:



Date: 3/18/2025

Office of the Tehama County Counsel
Margaret Long, County Counsel