

Attachment B

Alcor Solutions Inc

Managed Services FY

2026-29

Board Contract # _____

**AGREEMENT FOR SERVICES OF
INDEPENDENT CONTRACTOR
BETWEEN
COUNTY OF SANTA BARBARA
AND
ALCOR SOLUTIONS, INC.
FOR
MANAGED SERVICES**

TABLE OF CONTENTS

STANDARD TERMS AND CONDITIONS 4

SIGNATURE PAGE 15

EXHIBIT A-1 STATEMENT OF WORK MANAGED SERVICES..... 17

EXHIBIT AA GENERAL PROVISIONS NON-DIRECT SERVICES 34

 EXHIBIT AA General Provisions Mental Health Plan Required Terms (Non-Direct Service Provider) 35

EXHIBIT AA – AA1 ATTACHMENT 1 &2 CERTIFICATION REGARDING LOBBYING..... 57

 Attachment 1 State of California Department of Health Care Services Certification Regarding Lobbying..... 58

 Attachment 2 Certification Regarding Lobbying 59

EXHIBIT AA-1 GENERAL PROVISIONS BEHAVIORAL HEALTH SERVICES ACT SERVICES (BHSA) . 62

 Exhibit AA-1 General Provisions Department of Health Care Services State Performance Requirements Behavioral Health Services Act (BHSA)..... 63

EXHIBIT B(S) FINANCIAL PROVISIONS NON-DIRECT SERVICES 67

 Exhibit B Financial Provisions 68

 Exhibit B-1 MHS Schedule of Rates and Contract Maximum 69

EXHIBIT C STANDARD INDEMNIFICATION AND INSURANCE PROVISIONS 71

 Exhibit C Indemnification and Insurance Requirements..... 72

EXHIBIT D HIPAA BUSINESS ASSOCIATE AGREEMENT (BAA) 76

 EXHIBIT BAA HIPAA BUSINESS ASSOCIATE AGREEMENT (version 9.25.24) 77

STANDARD TERMS **AND CONDITIONS**

**AGREEMENT
FOR SERVICES OF INDEPENDENT CONTRACTOR**

THIS AGREEMENT (hereafter Agreement) is made by and between the County of Santa Barbara, a political subdivision of the State of California (hereafter COUNTY) and Alcor Solutions, Inc. with an address at 7600 Dublin Blvd, Suite 230, Dublin, CA 94568 (hereafter CONTRACTOR) wherein CONTRACTOR agrees to provide and COUNTY agrees to accept the services specified herein.

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

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

1. DESIGNATED REPRESENTATIVE.

Director at phone number 805-681-5220 is the representative of COUNTY and will administer this Agreement for and on behalf of COUNTY. Ziyang "Magic" Tan at phone number 949-335-8770 is the authorized representative for CONTRACTOR. Changes in designated representatives shall be made only after advance written notice to the other party.

2. NOTICES.

Any notice or consent required or permitted to be given under this Agreement shall be given to the respective parties in writing, by personal delivery or facsimile, or with postage prepaid by first class mail, registered or certified mail, or express courier service, as follows:

To COUNTY:

Director
COUNTY of Santa Barbara
Department of Behavioral Wellness
300 N. San Antonio Road
Santa Barbara, CA 93110
Fax: 805-681-5262

To CONTRACTOR:

Ziyang "Magic" Tan, Senior Principal & Customer Success
Alcor Solutions, Inc.
7600 Dublin Blvd, Suite 230
Dublin, CA 94568

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

3. SCOPE OF SERVICES.

CONTRACTOR agrees to provide services to COUNTY in accordance with EXHIBITS A(s) attached hereto and incorporated herein by reference.

4. TERM.

CONTRACTOR shall commence performance on July 1, 2026 and end performance upon completion, but no later than June 30, 2029 unless otherwise directed by COUNTY or unless earlier terminated.

5. COMPENSATION OF CONTRACTOR.

In full consideration for CONTRACTOR's services, CONTRACTOR shall be paid for performance under this Agreement in accordance with the terms of EXHIBIT B(s) attached hereto and incorporated herein by reference.

6. INDEPENDENT CONTRACTOR.

It is mutually understood and agreed that CONTRACTOR (including any and all of its officers, agents, and employees), shall perform all of its services under this Agreement as an independent contractor as to COUNTY and not as an officer, agent, servant, employee, joint venturer, partner, or associate of COUNTY. Furthermore, COUNTY shall have no right to control, supervise, or direct the manner or method by which CONTRACTOR shall perform its work and function. However, COUNTY shall retain the right to administer this Agreement so as to verify that CONTRACTOR is performing its obligations in accordance with the terms and conditions hereof. CONTRACTOR understands and acknowledges that it shall not be entitled to any of the benefits of a COUNTY employee, including but not limited to vacation, sick leave, administrative leave, health insurance, disability insurance, retirement, unemployment insurance, workers' compensation and protection of tenure. CONTRACTOR shall be solely liable and responsible for providing to, or on behalf of, its employees all legally-required employee benefits. In addition, CONTRACTOR shall be solely responsible and save COUNTY harmless from all matters relating to payment of CONTRACTOR's employees, including compliance with Social Security withholding and all other regulations governing such matters. It is acknowledged that during the term of this Agreement, CONTRACTOR may be providing services to others unrelated to the COUNTY or to this Agreement.

7. STANDARD OF PERFORMANCE.

CONTRACTOR represents that it has the skills, expertise, and licenses/permits necessary to perform the services required under this Agreement. Accordingly, CONTRACTOR shall perform all such services in the manner and according to the standards observed by a competent practitioner of the same profession in which CONTRACTOR is engaged. All products of whatsoever nature, which CONTRACTOR delivers to COUNTY pursuant to this Agreement, shall be prepared in a first class and workmanlike manner and shall conform to the standards of quality normally observed by a person practicing in CONTRACTOR's profession. CONTRACTOR shall correct or revise any errors or omissions, at COUNTY's request without additional compensation. Permits and/or licenses shall be obtained and maintained by CONTRACTOR without additional compensation.

8. DEBARMENT AND SUSPENSION.

CONTRACTOR certifies to COUNTY that it and its employees and principals are not debarred, suspended, or otherwise excluded from or ineligible for, participation in federal, state, or county government contracts. CONTRACTOR certifies that it shall not contract with a subcontractor that is so debarred or suspended. CONTRACTOR shall also comply with the debarment and suspension provisions set forth in Exhibit AA General Provisions Mental Health Plan Required Terms (Non-Direct Service Provider) and Exhibit AA-1 General Provisions Department of Health Care Services State Performance Requirements Behavioral Health Services Act (BHSA) o this Agreement.

9. TAXES.

CONTRACTOR shall pay all taxes, levies, duties, and assessments of every nature due in connection with any work under this Agreement and shall make any and all payroll deductions required by law. COUNTY shall not be responsible for paying any taxes on CONTRACTOR's behalf, and should COUNTY be required to do so by state, federal, or local taxing agencies, CONTRACTOR agrees to promptly reimburse COUNTY for the full value of such paid taxes plus interest and penalty, if any. These taxes shall include, but not be limited to, the following: FICA (Social Security), unemployment insurance contributions, income tax, disability insurance, and workers' compensation insurance.

10. CONFLICT OF INTEREST.

CONTRACTOR covenants that CONTRACTOR presently has no employment or interest and shall not acquire any employment or interest, direct or indirect, including any interest in any business, property, or source of income, which would conflict in any manner or degree with the performance of services required to be performed under this Agreement. CONTRACTOR further covenants that in the performance of this Agreement, no person having any such interest shall be employed by CONTRACTOR. CONTRACTOR must promptly disclose to COUNTY, in writing, any potential conflict of interest. COUNTY retains the right to waive a conflict of interest disclosed by CONTRACTOR if COUNTY determines it to be immaterial, and such waiver is only effective if

provided by COUNTY to CONTRACTOR in writing. CONTRACTOR shall also comply with the conflict of interest provisions set forth in Exhibit AA General Provisions Mental Health Plan Required Terms (Non-Direct Service Provider) and Exhibit AA-1 General Provisions Department of Health Care Services State Performance Requirements Behavioral Health Services Act (BHSA) to this Agreement.

11. OWNERSHIP OF DOCUMENTS AND INTELLECTUAL PROPERTY.

COUNTY shall be the owner of the following items incidental to this Agreement upon production, whether or not completed: all data collected, all documents of any type whatsoever, all photos, designs, sound or audiovisual recordings, software code, inventions, technologies, and other materials, and any material necessary for the practical use of such items, from the time of collection and/or production whether or not performance under this Agreement is completed or terminated prior to completion. CONTRACTOR shall not release any of such items to other parties except after prior written approval of COUNTY.

Unless otherwise specified in Exhibit A(s), CONTRACTOR hereby assigns to COUNTY all copyright, patent, and other intellectual property and proprietary rights to all data, documents, reports, photos, designs, sound or audiovisual recordings, software code, inventions, technologies, and other materials prepared or provided by CONTRACTOR pursuant to this Agreement (collectively referred to as "Copyrightable Works and Inventions"). COUNTY shall have the unrestricted authority to copy, adapt, perform, display, publish, disclose, distribute, create derivative works from, and otherwise use in whole or in part, any Copyrightable Works and Inventions. CONTRACTOR agrees to take such actions and execute and deliver such documents as may be needed to validate, protect and confirm the rights and assignments provided hereunder. CONTRACTOR warrants that any Copyrightable Works and Inventions and other items provided under this Agreement will not infringe upon any intellectual property or proprietary rights of any third party. CONTRACTOR at its own expense shall defend, indemnify, and hold harmless COUNTY against any claim that any Copyrightable Works or Inventions or other items provided by CONTRACTOR hereunder infringe upon intellectual or other proprietary rights of a third party, and CONTRACTOR shall pay any damages, costs, settlement amounts, and fees (including attorneys' fees) that may be incurred by COUNTY in connection with any such claims. This Ownership of Documents and Intellectual Property provision shall survive expiration or termination of this Agreement.

12. NO PUBLICITY OR ENDORSEMENT.

CONTRACTOR shall not use COUNTY's name or logo or any variation of such name or logo in any publicity, advertising or promotional materials. CONTRACTOR shall not use COUNTY's name or logo in any manner that would give the appearance that the COUNTY is endorsing CONTRACTOR. CONTRACTOR shall not in any way contract on behalf of or in the name of COUNTY. CONTRACTOR

shall not release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning the COUNTY or its projects, without obtaining the prior written approval of COUNTY.

13. COUNTY PROPERTY AND INFORMATION.

All of COUNTY's property, documents, and information provided for CONTRACTOR's use in connection with the services shall remain COUNTY's property, and CONTRACTOR shall return any such items whenever requested by COUNTY and whenever required according to the Termination section of this Agreement. CONTRACTOR may use such items only in connection with providing the services. CONTRACTOR shall not disseminate any COUNTY property, documents, or information without COUNTY's prior written consent.

14. RECORDS, AUDIT, AND REVIEW.

CONTRACTOR shall keep such business records pursuant to this Agreement as would be kept by a reasonably prudent practitioner of CONTRACTOR's profession and shall maintain such records for at least four (4) years following the termination of this Agreement. All accounting records shall be kept in accordance with generally accepted accounting principles. COUNTY shall have the right to audit and review all such documents and records at any time during CONTRACTOR 's regular business hours or upon reasonable notice. In addition, if this Agreement exceeds ten thousand dollars (\$10,000.00), CONTRACTOR shall be subject to the examination and audit of the California State Auditor, at the request of the COUNTY or as part of any audit of the COUNTY, for a period of three (3) years after final payment under the Agreement (Cal. Govt. Code Section 8546.7). CONTRACTOR shall participate in any audits and reviews, whether by COUNTY or the State, at no charge to COUNTY.

If federal, state, or COUNTY audit exceptions are made relating to this Agreement, CONTRACTOR shall reimburse all costs incurred by federal, state, and/or COUNTY governments associated with defending against the audit exceptions or performing any audits or follow-up audits, including but not limited to: audit fees, court costs, attorneys' fees based upon a reasonable hourly amount for attorneys in the community, travel costs, penalty assessments and all other costs of whatever nature. Immediately upon notification from COUNTY, CONTRACTOR shall reimburse the amount of the audit exceptions and any other related costs directly to COUNTY as specified by COUNTY in the notification.

CONTRACTOR shall also comply with the records, audit and review provisions set forth in Exhibit AA General Provisions Mental Health Plan Required Terms (Non-Direct Service Provider) and Exhibit AA-1 General Provisions Department of Health Care Services State Performance Requirements Behavioral Health Services Act (BHSA) to this Agreement.

15. INDEMNIFICATION AND INSURANCE.

CONTRACTOR agrees to and shall comply with the indemnification and insurance provisions as set forth in EXHIBIT C attached hereto and incorporated herein by reference.

16. NONDISCRIMINATION.

COUNTY hereby notifies CONTRACTOR that COUNTY's Unlawful Discrimination Ordinance (Article XIII of Chapter 2 of the Santa Barbara COUNTY Code) applies to this Agreement and is incorporated herein by this reference with the same force and effect as if the ordinance were specifically set out herein and CONTRACTOR agrees to comply with said ordinance. CONTRACTOR shall also comply with the nondiscrimination provisions set forth in Exhibit AA General Provisions Mental Health Plan Required Terms (Non-Direct Service Provider) and Exhibit AA-1 General Provisions Department of Health Care Services State Performance Requirements Behavioral Health Services Act (BHSA) to this Agreement.

17. NONEXCLUSIVE AGREEMENT.

CONTRACTOR understands that this is not an exclusive Agreement and that COUNTY shall have the right to negotiate with and enter into contracts with others providing the same or similar services as those provided by CONTRACTOR as the COUNTY desires.

18. NON-ASSIGNMENT.

CONTRACTOR shall not assign, transfer or subcontract this Agreement or any of its rights or obligations under this Agreement without the prior written consent of COUNTY and any attempt to so assign, subcontract or transfer without such consent shall be void and without legal effect and shall constitute grounds for termination.

19. TERMINATION.

A. **By COUNTY.** COUNTY may, by written notice to CONTRACTOR, terminate this Agreement in whole or in part at any time, whether for COUNTY's convenience, for nonappropriation of funds, or because of the failure of CONTRACTOR to fulfill the obligations herein.

1. **For Convenience.** COUNTY may terminate this Agreement in whole or in part upon 30 days written notice. During the thirty (30) day period, CONTRACTOR shall, as directed by COUNTY, wind down and cease its services as quickly and efficiently as reasonably possible, without performing unnecessary services or activities and by minimizing negative effects on COUNTY from such winding down and cessation of services.

2. **For Nonappropriation of Funds.** Notwithstanding any other provision of this Agreement, in the event that no funds or insufficient funds are appropriated or

budgeted by federal, state or COUNTY governments, or funds are not otherwise available for payments in the fiscal year(s) covered by the term of this Agreement, then COUNTY will notify CONTRACTOR of such occurrence and COUNTY may terminate or suspend this Agreement in whole or in part, with or without a prior notice period. Subsequent to termination of this Agreement under this provision, COUNTY shall have no obligation to make payments with regard to the remainder of the term.

- 3. For Cause.** Should CONTRACTOR default in the performance of this Agreement or materially breach any of its provisions, COUNTY may, at COUNTY's sole option, terminate or suspend this Agreement in whole or in part by written notice. Upon receipt of notice, CONTRACTOR shall immediately discontinue all services affected (unless the notice directs otherwise) and notify COUNTY as to the status of its performance. The date of termination shall be the date the notice is received by CONTRACTOR, unless the notice directs otherwise.
- B. By CONTRACTOR.** Should COUNTY fail to pay CONTRACTOR all or any part of the payment set forth in EXHIBIT B(s), CONTRACTOR may, at CONTRACTOR's option terminate this Agreement if such failure is not remedied by COUNTY within 30 days of written notice to COUNTY of such late payment.
- C.** Upon termination, CONTRACTOR shall deliver to COUNTY all data, estimates, graphs, summaries, reports, and all other property, records, documents or papers as may have been accumulated or produced by CONTRACTOR in performing this Agreement, whether completed or in process, except such items as COUNTY may, by written permission, permit CONTRACTOR to retain. Notwithstanding any other payment provision of this Agreement, COUNTY shall pay CONTRACTOR for satisfactory services performed to the date of termination to include a prorated amount of compensation due hereunder less payments, if any, previously made. In no event shall CONTRACTOR be paid an amount in excess of the full price under this Agreement nor for profit on unperformed portions of service. CONTRACTOR shall furnish to COUNTY such financial information as in the judgment of COUNTY is necessary to determine the reasonable value of the services rendered by CONTRACTOR. In the event of a dispute as to the reasonable value of the services rendered by CONTRACTOR, the decision of COUNTY shall be final. The foregoing is cumulative and shall not affect any right or remedy which COUNTY may have in law or equity.

20. SECTION HEADINGS.

The headings of the several sections, and any Table of Contents appended hereto, shall be solely for convenience of reference and shall not affect the meaning, construction or effect hereof.

21. SEVERABILITY.

If any one or more of the provisions contained herein shall for any reason be held to be invalid, illegal or unenforceable in any respect, then such provision or provisions shall be deemed severable from the remaining provisions hereof, and such invalidity, illegality or unenforceability shall not affect any other provision hereof, and this Agreement shall be construed as if such invalid, illegal or unenforceable provision had never been contained herein.

22. REMEDIES NOT EXCLUSIVE.

No remedy herein conferred upon or reserved to COUNTY is intended to be exclusive of any other remedy or remedies, and each and every such remedy, to the extent permitted by law, shall be cumulative and in addition to any other remedy given hereunder or now or hereafter existing at law or in equity or otherwise.

23. TIME IS OF THE ESSENCE.

Time is of the essence in this Agreement and each covenant and term is a condition herein.

24. NO WAIVER OF DEFAULT.

No delay or omission of COUNTY to exercise any right or power arising upon the occurrence of any event of default shall impair any such right or power or shall be construed to be a waiver of any such default or an acquiescence therein; and every power and remedy given by this Agreement to COUNTY shall be exercised from time to time and as often as may be deemed expedient in the sole discretion of COUNTY.

25. ENTIRE AGREEMENT AND AMENDMENT.

In conjunction with the matters considered herein, this Agreement contains the entire understanding and agreement of the parties and there have been no promises, representations, agreements, warranties or undertakings by any of the parties, either oral or written, of any character or nature hereafter binding except as set forth herein. This Agreement may be altered, amended or modified only by an instrument in writing, executed by the parties to this Agreement and by no other means. Each party waives their future right to claim, contest or assert that this Agreement was modified, canceled, superseded, or changed by any oral agreements, course of conduct, waiver or estoppel. Any requests for changes to this Agreement by CONTRACTOR shall be in writing and submitted to COUNTY before April 1 of the fiscal year for which the change would be applicable. Requests for changes failing to meet these requirements will not be considered. Notwithstanding any other provision of this Agreement, immaterial changes (such as changes to the Designated Representatives or addresses for purposes of Notice) as well as changes to this Agreement specified in the Exhibits may be authorized by the Director of the Department of Behavioral Wellness or designee in writing. These changes shall apply without the

need for an amendment of this Agreement executed by the parties. All other changes shall be made by an amendment of this Agreement in compliance with this Section.

26. SUCCESSORS AND ASSIGNS.

All representations, covenants and warranties set forth in this Agreement, by or on behalf of, or for the benefit of any or all of the parties hereto, shall be binding upon and inure to the benefit of such party, its successors and assigns.

27. COMPLIANCE WITH LAW.

CONTRACTOR shall, at its sole cost and expense, comply with all federal, state, and local statutes; ordinances; regulations; orders including, but not limited to, executive orders, court orders, and health officer orders; policies; guidance; bulletins; information notices; and letters including, but not limited to, those issued by the California Department of Health Care Services (DHCS) now in force or which may hereafter be in force with regard to this Agreement. The judgment of any court of competent jurisdiction, or the admission of CONTRACTOR in any action or proceeding against CONTRACTOR, whether COUNTY is a party thereto or not, that CONTRACTOR has violated any such statute, ordinance, regulation, order, policy, guidance, bulletin, information notice, and/or letter shall be conclusive of that fact as between CONTRACTOR and COUNTY.

28. CALIFORNIA LAW AND JURISDICTION.

This Agreement shall be governed by the laws of the State of California. Any litigation regarding this Agreement or its contents shall be filed in the County of Santa Barbara, if in state court, or in the federal district court nearest to Santa Barbara County, if in federal court.

29. EXECUTION OF COUNTERPARTS.

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

30. AUTHORITY.

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

31. SURVIVAL.

All provisions of this Agreement which by their nature are intended to survive the termination or expiration of this Agreement shall survive such termination or expiration.

32. PRECEDENCE.

In the event of conflict between the provisions contained in the numbered sections of this Agreement and the provisions contained in the Exhibits, the provisions of the Exhibits shall prevail over those in the numbered sections.

33. BUSINESS ASSOCIATE.

The parties agree to the terms and conditions set forth in Exhibit D – HIPAA Business Associate Agreement (BAA), attached hereto and incorporated herein by reference.

THIS SECTION LEFT BLANK INTENTIONALLY.

SIGNATURE PAGE FOLLOWS.

SIGNATURE PAGE

SIGNATURE PAGE

Agreement for Services of Independent Contractor between the **County of Santa Barbara** and **Alcor Solutions, Inc.**

IN WITNESS WHEREOF, the parties have executed this Agreement to be effective on July 1, 2026.

COUNTY OF SANTA BARBARA

By: _____
BOB NELSON, CHAIR
BOARD OF SUPERVISORS

Date: _____

ATTEST:

MONA MIYASATO
COUNTY EXECUTIVE OFFICER
CLERK OF THE BOARD

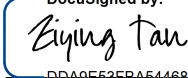
By: _____

Deputy Clerk

Date: _____

CONTRACTOR:

ALCOR SOLUTIONS, INC.

By:  _____
Authorized Representative

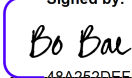
Name: Ziying Tan

Title: Principal

Date: 6/10/2026

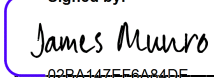
APPROVED AS TO FORM:

RACHEL VAN MULLEM
COUNTY COUNSEL

By:  _____
Deputy County Counsel

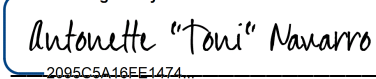
APPROVED AS TO ACCOUNTING FORM

BETSY M. SCHAFFER, CPA
AUDITOR-CONTROLLER

By:  _____
Deputy

RECOMMENDED FOR APPROVAL:

ANTONETTE NAVARRO, LMFT DIRECTOR,
DEPARTMENT OF BEHAVIORAL WELLNESS

By:  _____
Director

APPROVED AS TO FORM:

MARISA KAHN, RISK MANAGER,
RISK MANAGEMENT

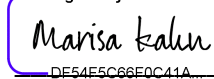
By:  _____
Risk Manager

EXHIBIT A-1
STATEMENT OF WORK
MANAGED SERVICES

MANAGED SERVICES ENGAGEMENT OVERVIEW

SCOPE

Santa Barbara County Department of Behavioral Wellness (Department) has implemented ServiceNow as the enterprise platform of choice for service management. As a part of this engagement, Department is looking to leverage the Alcor Managed Services team for ongoing ServiceNow platform support & maintenance activities.

Based on the prioritization of Department, Alcor will provide the managed services support-related applications and functions implemented within ServiceNow including, but not limited to, the following:

- Form Configuration (UI Changes)
- List Configuration
- Exporting Data
- Importing Data (transform maps)
- Create & scheduling of reports & dashboards
- Creating/Maintaining Roles
- Creating/Maintaining Users and Associating to Groups
- Creating/Maintaining Groups
- Customization of the UI Appearance
- Addition of single, independent variables to catalog
- Database views for reporting
- Modification of client scripts and business rules
- Catalog item build and maintenance
- Configuring and Maintaining Access Control Lists (ACLs)
- Service Portal (e.g., branding, layout, UI/UX Design Expertise)

SERVICES

Alcor will perform the following Services:

- Training and Organizational Change Management/Communications assistance for any ServiceNow or Enterprise Service Management activities needed.
- Work in descending order of priority as notated within Department's Demand and Enhancement records (e.g., P1, P2, P3, etc.).
- Application specific system administration.
- ServiceNow best practice development practices.
- Unit and functional test all developed code.
- Populate all required information pertinent to the development into the ticket, including any relevant knowledge transfer.
- Reassign all requests, tickets, etc. back to requestor for proper User Acceptance Testing.
- Provide support during code promotion to higher environments.
- Provide Knowledge Transfer of developed items.
- Provide advice and guidance to Department's key contacts on the appropriate use of the platform, processes, and procedures.
 - One (1) major environment upgrade will be supported per year as part of the scope of managed services.
 - Reporting: Alcor will provide hours consumption monthly. These hours will be reported to Department stakeholders by the Alcor Engagement Manager to ensure future work and enhancements are triaged and scheduled in a manner which matches Department's desired budget and timelines.

Note:

- This statement of work includes defect and enhancement support for HR Service Delivery (HRSD). Defect and enhancement support for IT Service Management (ITSM), Contracts, and AccessFlow requires 6 weeks' notice to ensure resource availability.

Summary of Contract Services

- IT Consultant Services
 - Enhancements
 - Minimum billing amount: 2 Medium or 6 Small HRSD Enhancements Per Month

- Maximum billing amount: 1 Large or 3 Medium or 9 Small HRSD Enhancements Per Month
- Additional enhancements above the monthly “minimum billing amount” must be approved in writing by the Department’s Process Owners or Chief Information Officer (CIO).
- Additional enhancements above the monthly “maximum billing amount” will be billed on a Time and Materials basis at the rate specified in Exhibit B-1 (Schedule of Rates). Additional hours must have written approval by the Department’s Process Owners or CIO.
- Meetings
 - 1 Weekly HRSD Meeting
- Monitoring and remediation of HRSD Defects
- Quarterly Business Review Preparation and Execution
- One (1) Annual Upgrade: Additional time has been scoped specifically for upgrades to prevent the need for a development freeze for ITSM, HRSD, Contracts, and AccessFlow.
- Time and Materials
 - Alcor will provide Time and Material resources for as needed technical support for AccessFlow, ITSM, Asset Management, Contracts and other scope of Services with Department written approval. Time and Materials resources will be billed at the rate specified in Exhibit B-1 (Schedule of Rates) or based on specific project requirements. Additional hours or scope of work must have written approval by the Department’s Process Owners or CIO.

Alcor will provide the Services as follows:

- From a remote location
- From Department’s chosen location, as required

SERVICE HOURS

Alcor shall support Pacific hours by leveraging resources from onshore and offshore. Alcor will provide blended support coverage from the North America Pacific Standard Time & the India Standard Time (IST), except for North American and India statutory holidays. US operating hours will be 9:00am – 5:00pm (Pacific Time Zone) Monday-Friday. Any support required above the scoped hours in a given month will need to be pre-approved in writing by Department

Summer

	12:30	1:30	2:30	3:30	4:30	5:30	6:30	7:30	8:30	9:30	10:30	11:30	12:30	1:30	2:30	3:30	4:30	5:30
IST	PM	PM	PM	PM	PM	PM	PM	PM	PM	PM	PM	PM	AM	AM	AM	AM	AM	AM
	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00
EST	AM	AM	AM	AM	AM	AM	AM	AM	AM	PM	PM	PM	PM	PM	PM	PM	PM	PM
	12:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	1:00	2:00	3:00	4:00	5:00
PST	AM	AM	AM	AM	AM	AM	AM	AM	AM	AM	AM	AM	PM	PM	PM	PM	PM	PM

Winter - Day light saving

	1:30	2:30	3:30	4:30	5:30	6:30	7:30	8:30	9:30	10:30	11:30	12:30	1:30	2:30	3:30	4:30	5:30	6:30
IST	PM	PM	PM	PM	PM	PM	PM	PM	PM	PM	PM	AM	AM	AM	AM	AM	AM	AM
	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00
EST	AM	AM	AM	AM	AM	AM	AM	AM	AM	PM	PM	PM	PM	PM	PM	PM	PM	PM
	12:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	1:00	2:00	3:00	4:00	5:00
PST	AM	AM	AM	AM	AM	AM	AM	AM	AM	AM	AM	AM	PM	PM	PM	PM	PM	PM

LARGER SCOPE WORK

As requirements arise that would cause the monthly maximum to be exceeded to handle the work within the monthly scope, the Engagement Manager will work with Department’s stakeholders to determine how to best space out the work to accommodate the scoped hours as well as any other enhancements and operational support being worked simultaneously, or whether a Project Change Request or hourly overage is best suited to manage the work.

Some examples:

- Implementation of new Modules/applications (e.g., Major Incident or HRSD Case Management)
- Implementation of Integrations
- Exceptionally large catalog items with complex workflows
- Large/Major enhancements that would cause the monthly hour allocation to be exceeded if all pipelined enhancements were to be taken on simultaneously
- ServiceNow App Store plugin downloads and implementations

QUARTERLY BUSINESS REVIEW

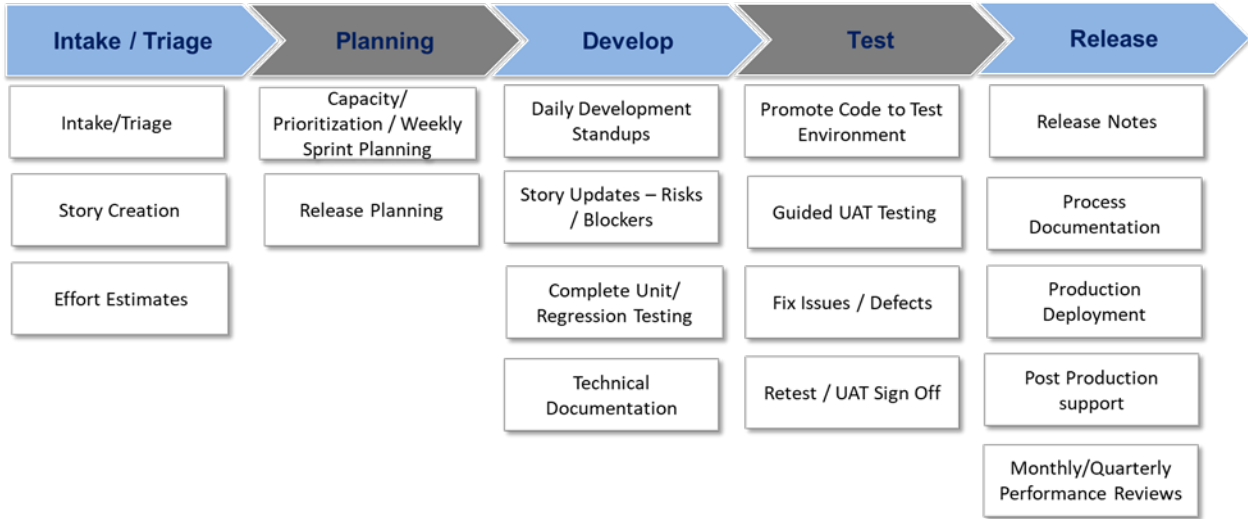
In addition to the weekly and monthly reporting on consumed hours and accomplished work, Department may, at its discretion, elect to participate in a formal Quarterly Business Review. Department must provide approval to initiate a formal Quarterly Business Review. Alcor recommends a formal Quarterly Business Review cadence be established to ensure:

- The Department stakeholders, both direct and indirect, are receiving all of the expected quality and quantity of delivery by the Alcor staff, taking time to identify specific areas of improvement or course-correction
- Mutual exchange of feedback on the relationship
- Overview of any RIDAC-type components that are within scope of the MSP's oversight
- Communication of upcoming key milestones or projects
- Opportunity for strategic discussions on this scope of work, or any other major client-side initiatives that may be of interest or may impact Alcor
- Adjustments needed to the scoped work or minimum hours allocated in this contract

For this Quarterly Business Review, Alcor will bring any necessary consultants to the table, as well as the Engagement Manager and the Alcor Executive Sponsor.

As an output of the Quarterly Business Review, should either party deem it necessary to request a change in the monthly minimum hours of the contract, the request may be made with at least 60 days' notice to yield a revised and signed contract.

MSP APPROACH AND METHODOLOGY



Activities

Incident Management: Once a ticket is categorized as an Incident, the Alcor developers will create a defect in Department’s ServiceNow Software Development Life Cycle (SDLC) application and commence work on the resolution. An iterative process will provide Department User Acceptance Testing until the issue has been resolved. Once resolved, all test cases will be submitted for approval and upon approval the fix will be pushed into Production on a continuous release cycle.

Small Enhancement Request(s): Once a request is categorized as an Enhancement Request, the Alcor consultant will work with the enhancement developer to review the requirements and provide effort estimates to Department. Once the estimate is approved by Department, the following activities will be conducted:

Release Planning

- Alcor’s standard is to have bi-monthly releases for Enhancement items
- Alcor will conduct release planning meetings with Department every Thursday unless otherwise agreed upon.
- During the Release Planning meeting, the parties agree that the following will happen:
- Department provides input on the priority of the requests.
- Alcor will assess its team’s capacity to deliver against the prioritized backlog.

- Department and Alcor will mutually agree on the recommended feature sets for each/next release.

Sprint Planning

- Once the release is determined, Alcor will conduct weekly sprint planning to define the sprints within the releases.
- The output of these is a clearly defined sprint plan to address all the feature sets within the next release.

Sprint Execution

- Weekly internal Unit & Functional testing
 - On a weekly basis, Alcor will conduct internal functional testing
 - This will also include a wider testing stance to include fully integrated system & functional testing based on the requirement requested.
 - Code Reviews: Alcor will conduct weekly code reviews with a Senior Developer. All requirements will be discussed with the developer explaining the logic / approach and testing components validating best practice and NOW (ServiceNow) standards are followed.
 - For the stories that pass the internal functional & system testing, they will be submitted to Department for User Acceptance Testing. For the stories that fail the testing, they will be put back in the backlogs

Release

- Alcor support analyst will develop release notes and publish them to Department after the releases are pushed into production successfully.

Emergency Releases

- During Department business hours, an emergency release will be any incident or enhancement that requires immediate deployment to “fix” or restore service to a normal state.
- Emergency releases will require a Change ticket with proper approval levels.
- The Alcor developer will review and resolve any errors if applicable, provide post-production deployment support, and develop release notes and publish them to Department after the releases are pushed into production successfully.

RESOURCES

The parties expect the following resources to be engaged from Department and Alcor for this engagement. The exact duration and level of engagement for Department resources will be finalized at kick-off.

Department Resources	Responsibilities
System Administrator	Administrator training must be completed by Department’s assigned resource(s) no later than the beginning of the Prepare stage.
Process Owner(s)	Department will provide subject matter experts who will be responsible for the correct and complete definition of each of the processes implemented within the ServiceNow product.
UAT Tester(s)	Department will provide UAT tester(s) who will be responsible for executing UAT test cases.

Alcor Resources	Responsibilities
Developer(s)	The developer(s) will handle all tooling configurations and unit testing that is captured in the enhancements backlog and will also be responsible for monitoring the instances to ensure Incidents and Problems are promptly resolved, if ever they arise.
Process and Tooling Consultants / Business System Analyst (BSA)	Ensures that the business process requirements are accurately reflected in ServiceNow capabilities. They serve as Subject Matter Experts (SMEs) for each process area bringing knowledge of best practice to provide ample consultation and ensure the business is informed in all decisions impacting the ServiceNow Platform.
Engagement Manager	Serves as the day-to-day Alcor peer to the Department Process Owners. They are the main point of contact for all efforts executed across the engagement. They will be accountable the creation and ongoing maintenance of the engagement project plan and demand pipeline. This person is responsible for all demand from an idea to stabilization in operations including the status and progress of all work, assigning of resources, managing change to time, budget and scope and communicating to client leadership. This role will also serve as the Senior ServiceNow Tooling and Process consultant advising on enhancements as required.

At a summary level, the Consultant/BSA, Developer, and Engagement Manager will proactively manage all aspects of the ServiceNow platform with maximum autonomy. Any activities pertaining to the management of the platform, ongoing consultation regarding the tooling or processes, and holistic oversight and reporting of the performance of this team, will be

considered in-scope for this statement of work. To give specifics on the bare minimum responsibilities of each of the three scoped roles, please see the below listing.

- Consultant / BSA
 - Daily
 - Review the progress for list of deliverables for the week and provide updates wherever relevant.
 - Complete Testing and enable development as and when enhancements /issues require the operations.
 - Provide communication to the Team (internal and to Department) on High priority items and any concerns.
 - Identify questions/clarifications that are needed by Department stakeholders and provide the responses needed.
 - Write stories for the development team.
 - Weekly/Bi-weekly
 - Execute requirements/sprint planning meetings with Department stakeholders and provide clear visibility on the planned activities for the sprint.
 - Update the decisions made into the application and enable appropriate assignments, priority, and estimate.
 - Drive the progress of the deliverable through instances Dev-test-prod by working with Department stakeholders on the User Acceptance Testing Process
 - Provide test plans, rollback plans for the change requests raised for production updates.
 - Report weekly hours for the time spent on the activities.
 - Provide documentation
 - Process/product - on the completed work to be added to the knowledge base for review.
 - End user instructions.
 - Monthly
 - Monitor the rate of completion and accuracy for each sprint and gather insights into future scope and integrate into backlog.

- Plan and project a scope and vision for the product while keeping the Process Owners in the loop for highest adoption.
- Raise and enable highest levels of communication to the leadership team with a clear indication of the path forward.
- Anticipate and plan for future patches and releases that must be included in the upcoming sprints.
- Anticipate and plan for increased need for Department stakeholders-side involvement including requirements gathering, testing, training, and OCM.
- Quarterly
 - Check the goals accomplished and review the lessons learned.
 - Drive Product roadmap discussions and review upcoming versions of ServiceNow for consolidation.
 - Supply all performance data and forecasted demands and large upcoming projects for the Quarterly Business Review.
- Developer
 - Daily
 - Attend daily SCRUM meetings and identify blockers for weekly deliverable goals.
 - Work on stories and update according to the status.
 - Provide technical clarifications on issues raised including root cause analysis.
 - Drive Unit testing for the changes that are done and retest after fixes are applied.
 - Weekly/Bi-weekly
 - Participate in release planning discussions to provide estimates for the stories (enhancements/defects).
 - Report weekly hours on the time spent on development per story (enhancement/issue).
 - Conduct code migration activities between instances (DEV-TEST-PROD) as dictated by the status of the stories.
 - Provide Update set information for change requests raised.

- Provide technical documentation and assistance wherever required.
- Monthly
 - Participate in feedback planning discussions to guide the consultation on grooming the backlog.
 - Conduct cloning activities between instances (DEV-TEST-PROD) as dictated by best practices.
 - Drive monthly releases as required based on the scheduled sprints.
- Quarterly
 - Provide technical input to the team to drive product vision conversations.
 - Enable upgrade conversations and provide technical insight into upcoming features and complexity involved.
 - Track Patch upgrades as they happen and enable smooth consolidation into existing backlog by syncing up with the consultant and Department stakeholders.
- Engagement Manager
 - Weekly
 - Reporting on projected versus consumed hours and advising on actions required based on RIDAC contents and weekly feedback.
 - Accountable for the lock-step coordination and communication between all Alcor engagements (e.g., Managed Services as well as Projects and PCRs).
 - Monthly
 - Review of completed scope from past month and an overview of upcoming demand for the future month.
 - Anticipating and preparing for larger bodies of work, such as major upgrades, large enhancements, platform expansions.
 - Quarterly
 - Coordinating the Quarterly Business Reviews where executive leadership from both organizations will convene to discuss overall program status, exchange feedback, and plan for future bodies of work.

RESOURCE RACI CHART

Responsibility	Department	Alcor
Establish a formal governance model to capture, review and prioritize ServiceNow implementation scope	RA	RC
Capture and document all process requirements pertaining to the proposed scope	RA	RC
Provide existing data in an error-free, comprehensive and ServiceNow supported mode	RA	C
Setup implementation infrastructure and onsite presence	C	RA
Provide a single point of contact for each in-scope process (Process Owner). This person will have accountability for approving enhancements and defects logged against the respective process	RA	RC
Define acceptance and exit criteria	RA	R
Provide UAT testers and execute User Acceptance Testing	RA	C
Perform training, implementation activities and transition to Production instance for all in-scope modules	C	AR
Lead working sessions, sprints, and release schedule	RA	RC
Deliver configuration and code sets to meet story acceptance criteria	C	AR

R – RESPONSIBLE: A – ACCOUNTABLE: C – CONSULT: I – INFORM

VELOCITY METRICS

Objective – Measure volume of work that can be delivered in a fixed interval. Alcor would like to establish the true baseline to these metrics during the initial 3 months period of this contract and establish the productivity gain goals for future years.

Number of enhancements / Service Requests delivered per month will be determined based on the urgency and impact or complexity of request.

Key Metrics	Measurement	Measurement Interval	Target (Monthly)	Benefit
# of HR Enhancement Features Delivered	# of HR enhancement requests delivered on a monthly basis	Monthly	2 Medium or 6 Small	<ul style="list-style-type: none"> Establish current velocity baseline Ability to set expectations with business – If business requires higher velocity, Alcor can deliver with additional staffing Ability to measure productivity and ongoing productivity improvement

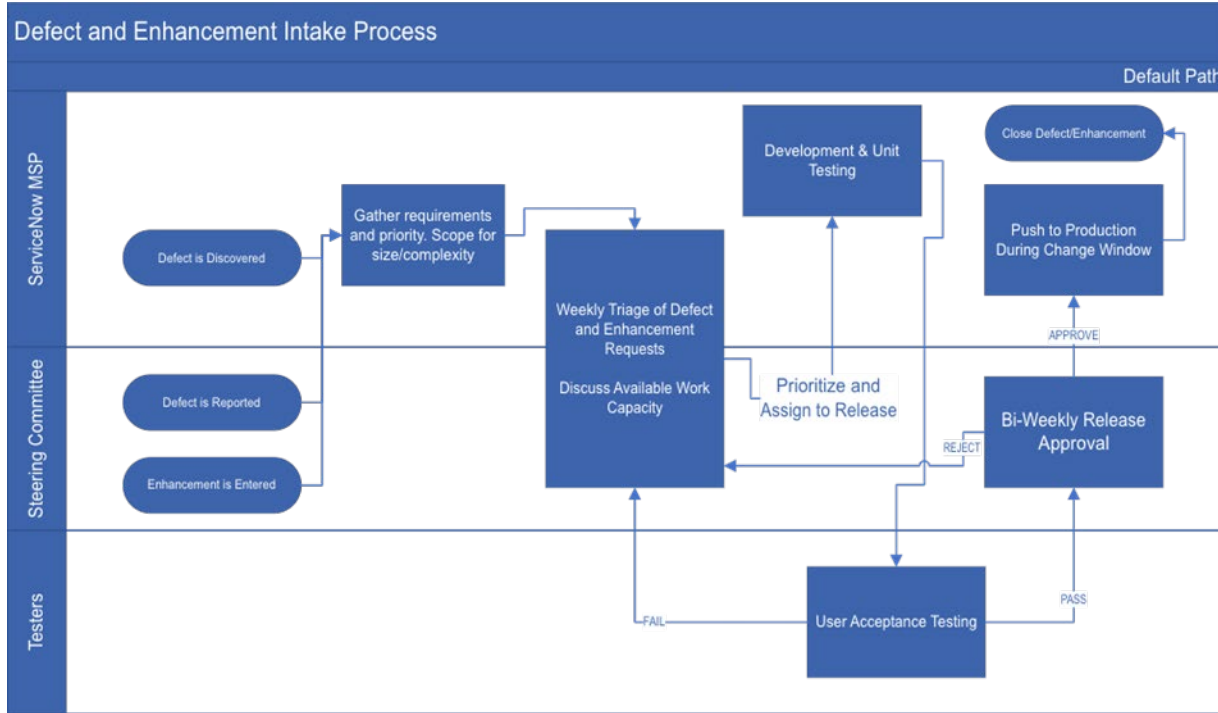
Sizing Definition and Assumptions

of HR Enhancement Request Delivered

		Complexity/Impact		
		High	Medium	Low
Urgency	High (<2 weeks)	large	large	medium
	Medium (2-4 weeks)	large	medium	small
	Low (>4 weeks)	medium	medium	small

- Required Capacity to Deliver (hours)
 - Large – 45
 - Medium – 15
 - Small: - 5
- One Large Request equals 3 Medium Requests
- One Medium Request equals 3 Small Requests
- Baseline capacity to include 30% resource to perform the following functions in support of Configuration Management:
 - Attend Department stakeholder meetings
 - Provide reporting
 - Intake requests, triage and classify requests
 - Communicate to Process Owners the status of their request
 - Incident management
- Sample Requests by Size
 - Large: Configuring a new portal
 - Medium: Altering HR case workflows to modify approver or fulfiller tasks
 - Small: Adding an existing field to a table or form.

If these factors impact resourcing overages by 5% or more within a given quarter, Alcor and Department will have an opportunity to true-up resourcing for capacity management. Any baseline shall not be changed without discussion and negotiating an adjustment to scope and fees via the change request process. Alcor Engagement manager will work with Department key stakeholders to project the work monthly so that appropriate additional capacity can be arranged if required.



ENGAGEMENT ASSUMPTIONS

Department acknowledges that its participation and cooperation is critical for the success of the Project. The following assumptions are based on information provided by Department to Alcor relating to the engagement scope and Department current business processes as of the Effective Date of this Agreement and have been used to compute the estimated level of effort and cost. Deviations from these assumptions may lead to commensurate changes in the timeline and fees, and such changes shall be mutually agreed by the parties through an amendment of this Agreement.

GENERAL

- a) The Alcor team will work directly with the client in requirements gathering, development status, ad-hoc meetings as required, testing, UAT support, production release(s) and weekly status meetings.
- b) Department will provide the required resources and ensure active participation to ensure the implementation is successful. This will include an executive decision-maker, project leadership and management, subject matter experts, and technical resources.
- c) Department is responsible for the definition of the business processes within scope for this Project and implementing all business process changes required to support the Project.
- d) Department is responsible for testing prior to production deployment.
- e) It is assumed that the Alcor resources will have remote access to Department's instances and that Department provides appropriate technologies for remote work.
- f) These timelines and effort estimates are based on staying close to out of the box functionality of ServiceNow and with limited added scripting/coding. Alcor will advise Department if any such scripting may require additional effort to build, review and test a given module.

EXHIBIT AA
GENERAL PROVISIONS
NON-DIRECT SERVICES

EXHIBIT AA
GENERAL PROVISIONS
MENTAL HEALTH PLAN REQUIRED TERMS
(NON-DIRECT SERVICE PROVIDER)

The following provisions shall apply to all services under this Agreement, included as Exhibit A-1, as though separately set forth in the scope of work specific to each service.

1. PERFORMANCE.

- A.** This Agreement shall be governed by, and construed in accordance with, all laws and regulations and all contractual obligations of County under the Integrated Intergovernmental Agreement (Contract No. 24-40145) between County and the California Department of Health Care Services (DHCS) including the federal and state requirements listed in Integrated Intergovernmental Agreement, Exhibit E (Additional Provisions), section 7 (State and Federal Laws Governing this Contract) and contractual obligations in Integrated Intergovernmental Agreement, Exhibit D (Special Terms and Conditions). The Integrated Intergovernmental Agreement, available at [County of Santa Barbara - File #: 25-00016](#), is incorporated herein by reference.
- 1.** Contractor agrees to comply with all applicable federal, state, and local laws including federal and state laws pertaining to member rights, applicable sections of California's Medicaid State Plan (State Plan), applicable federal waivers, and applicable DHCS Behavioral Health Information Notices (BHINs) in its provision of services as a subcontractor or contracted provider of County as an integrated county behavioral health plan.
 - 2.** Contractor agrees to perform all applicable delegated activities and obligations including services and reporting responsibilities in compliance with County's obligations under the Integrated Intergovernmental Agreement.
 - 3.** Contractor agrees to comply with any changes to these statutes and regulations, State Plan, federal waivers, or BHINs or any amendments to the Integrated Intergovernmental Agreement that occur during the Term of this Agreement. Contractor shall also comply with any newly applicable statute, regulation, State Plan Amendment, federal waiver, and BHIN that become effective during the Term of this Agreement. These obligations shall apply without the need for an amendment(s) of this Agreement. If the parties amend the affected provisions of this Agreement to conform to the changes in law or the Integrated

Intergovernmental Agreement, the amendment shall be retroactive to the effective date of such changes in law or the Integrated Intergovernmental Agreement.

4. To the extent there is a conflict between a provision of this Agreement and any federal, state, or local statute or regulation, State Plan, federal waiver, or BHIN or provision of the Integrated Intergovernmental Agreement, Contractor shall comply with the federal, state, or local statute or regulation, State Plan, federal waiver, or BHIN or provision of the Integrated Intergovernmental Agreement, and the conflicting provision of this Agreement shall no longer be in effect.

B. Contractor shall comply with the following as applicable:

1. All Medicaid laws, regulations including sub-regulatory guidance, and contract provisions;
2. 42 C.F.R. § 438.900 et seq. regarding parity in mental health and substance use disorder benefits;
3. All laws and regulations relating to patients' rights including Welfare and Institutions Code section 5325, 9 California Code of Regulations sections 862 through 868, and 42 Code of Federal Regulations section 438.100; and
4. All existing policy letters issued by DHCS. All policy letters issued by DHCS subsequent to the effective date of this Agreement shall provide clarification of Contractor's obligations pursuant to this Agreement.

C. Contractor shall comply with:

1. All applicable Behavioral Health Services Act laws, regulations, BHINs, policy letters, and guidance; and
2. The Santa Barbara County Mental Health Services Act Steering Committee Mission Statement, available at [Mental Health Services Act Steering Committee | Santa Barbara County, CA - Official Website](#).

D. **Suspension For Convenience**. The Director of the Department of Behavioral Wellness or designee may, without cause, order Contractor in writing to suspend, delay, or interrupt the services under this Agreement in whole or in part for up to 120 days. County shall incur no liability for suspension under this provision and suspension shall not constitute a breach of this Agreement.

2. CONFIDENTIALITY.

- A.** Contractor agrees, and shall require its employees, agents, subcontractors, or contracted providers to agree, to maintain the confidentiality of patient records pursuant to: Title 42 United State Code (USC) Section 290 dd-2; Title 42 Code of Federal Regulations (C.F.R.), Part 2; Title 42 C.F.R. Section 438.224; 45 C.F.R. Section 96.132(e), 45 C.F.R. Parts 160, 162, and 164; Title 22 California Code of Regulations (CCR) Section 51009; Welfare & Institutions Code (W&IC) Section 5328 et seq. and Sections 14100.2 and 14184.102; Health and Safety Code (HSC) Sections 11812 and 11845.5; Civil Code Sections 56 – 56.37, 1798.80 – 1798.82, and 1798.85; Integrated Intergovernmental Agreement Exhibit A—Attachment 4 (Management Information Systems), Section 6 (HIPAA and Additional Data Standards), Exhibit D, Section 14 (Confidentiality of Information), and Exhibit F (Business Associate Addendum); and this Agreement, Section F (Compliance with Privacy Laws and Data Security Authorities), as applicable. Patient records must comply with all applicable state and federal requirements.
- B.** Contractor shall ensure that no list of persons receiving services under this Agreement is published, disclosed, or used for any purpose except for the direct administration of services under this Agreement or other uses authorized by law that are not in conflict with requirements for confidentiality contained in the preceding codes.
- C.** Contractor shall comply with Exhibit F to the Integrated Intergovernmental Agreement to the extent Contractor is provided Personal Health Information (“PHI”), Personal Information (“PI”), or Personally Identifiable Information (“PII”) as defined in Exhibit F of the Integrated Intergovernmental Agreement from County to perform functions, services, or activities specified in this Agreement.
- D.** Contractor shall make itself and any subcontractors, employees or agents assisting Contractor in the performance of its obligations under this Agreement, available to County or DHCS at no cost to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against County, DHCS, its directors, officers or employees based upon claimed violations of privacy involving inactions or actions by Contractor, except where Contractor or its subcontractor, employee or agent is a named adverse party.
- E.** Upon termination or expiration of this Agreement for any reason, Contractor shall return or destroy all PHI, PI and PII accessed in a database maintained by County, received by Contractor from County, or acquired or created by Contractor in connection with performing functions, services, or activities specified in this Agreement on behalf of County that Contractor still maintains in any form, and shall

retain no copies of such PHI, PI or PII. If return or destruction is not feasible, Contractor shall notify County of the conditions that make the return or destruction infeasible, and County and Contractor shall determine the terms and conditions under which Contractor may retain the PHI, PI or PII. Contractor shall continue to extend the protections of Exhibit F of the Integrated Intergovernmental Agreement to such 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 subsection shall also apply to Department PHI, PI and PII that is in the possession of subcontractors or agents of Contractor.

- F. Compliance with Privacy and Data Security Authorities.** Contractor shall, at its sole cost and expense, comply with all applicable federal, state, and County healthcare privacy and data security requirements and authorities including, but not limited to, those authorities specified in Section 2.A of this EXHIBIT AA General Provisions Mental Health Plan Required Terms (Non-Direct Service Provider) now in force or which may hereafter be in force and shall develop and maintain comprehensive patient confidentiality policies and procedures, provide annual training of all staff regarding those policies and procedures, and demonstrate reasonable efforts to secure written and/or electronic data.

3. REPORTS.

- A.** Contractor agrees to submit data and reports as required by County or the California Department of Health Care Services (DHCS).
- B.** Contractor agrees that County or DHCS may withhold payments until Contractor has submitted any required data and reports to County or DHCS as identified in this Agreement, or Integrated Intergovernmental Agreement, Exhibit A(s) or Document 1F(a) Reporting Requirement Matrix for Counties.

4. MONITORING.

- A.** County shall monitor the performance of Contractor on an ongoing basis for compliance with the terms of the Integrated Intergovernmental Agreement and this Agreement. County shall assign senior management staff as contract monitors to coordinate periodic review meetings with Contractor's staff regarding quality of, fiscal and overall performance activity.
- B.** Contractor shall be liable to County for any penalties assessed against County for Contractor's failure to comply with the required corrective action.

5. ADDITIONAL PROGRAM REQUIREMENTS. (Reserved)

6. ADDITIONAL STATE CONTRACT COMPLIANCE REQUIREMENTS.

- A.** County and the California Department of Health Care Services (DHCS) may fully or partially revoke this Agreement or the delegated activities or obligations, or apply other remedies permitted by federal or state law when County or DHCS determine that Contractor has not performed satisfactorily (42 C.F.R. § 438.230(c)(2).)
- B.** Contractor shall comply with any applicable provision identified in the Integrated Intergovernmental Agreement as applying to subcontractors or contracted providers.
- C. Americans with Disabilities Act.** Contractor agrees to ensure that deliverables developed and produced pursuant to this Agreement shall comply with the accessibility requirements of sections 7405 and 11135 of the California Government Code, section 508 of the Rehabilitation Act of 1973 as amended (29 U.S.C. § 794d), regulations implementing the Rehabilitation Act of 1973 as set forth in part 1194 of title 36 of the Code of Federal Regulations, and the Americans with Disabilities Act of 1990 (42 U.S.C. § 12101 et seq.). In 1998, Congress amended the Rehabilitation Act of 1973 to require federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities. California Government Code sections 7405 and 11135 codify section 508 of the Rehabilitation Act of 1973 requiring accessibility of EIT.
- D. Generative Artificial Intelligence Technology Uses and Reporting.**
 - 1.** Contractor certifies its services or work under this Agreement does not include or make available any Generative Artificial Intelligence (GenAI) technology including GenAI from third parties or subcontractors.
 - 2.** During the Term of this Agreement, Contractor shall notify County in writing if its services or any work under this Agreement includes or makes available any previously unreported GenAI technology including GenAI from third parties or subcontractors. Contractor shall immediately complete the GenAI Reporting and Factsheet (STD 1000), available at [STD 1000 Generative Artificial Intelligence \(GenAI\) Disclosure & Factsheet](#) and submit the completed form to County to report the use of any new or previously unreported GenAI technology.
 - 3.** At the direction of County, Contractor shall discontinue the use of any new or previously undisclosed GenAI technology that materially impacts functionality, risk, or contract performance until use of such GenAI technology has been approved by County.

4. Contractor acknowledges and agrees that its failure to disclose GenAI technology use and submit the GenAI Reporting and Factsheet (STD 1000) to County may be considered a material breach of this Agreement by County or the California Department of Health Care Services (DHCS), and County or DHCS may consider the failure to disclose GenAI technology use and/or submit the [STD 1000 Generative Artificial Intelligence \(GenAI\) Disclosure & Factsheet.pdf](#) to County as grounds for the immediate termination of this Agreement. County and DHCS are entitled to seek all the relief to which they may be entitled as a result of such non-disclosure.
5. Contractor shall include subsection D ([Generative Artificial Intelligence Technology Uses and Reporting](#)) of this Section (Additional State Contract Compliance Requirements) in all subcontracts to perform work under this Agreement.

E. Prohibited Affiliations.

1. Contractor shall not knowingly have any prohibited type of relationship, as described in subsection E.3 of this Section 6 (Additional State Contract Compliance Requirements), with individuals or entities listed in subsection E.1.i and ii. Contractor shall further require that its subcontractors and contracted providers abide by this requirement.
 - i. An individual or entity that is debarred, suspended, or otherwise excluded from participating in procurement activities under the Federal Acquisition Regulation or from participating in non-procurement activities under regulations issued under Executive Order No. 12549 or under guidelines implementing Executive Order No. 12549. (42 C.F.R. § 438.610(a)(1).)
 - ii. An individual or entity who is an affiliate, as defined in the Federal Acquisition Regulation at 48 C.F.R. section 2.101, of a person described in subsection D.1.i. (42 C.F.R. § 438.610(a)(2).)
2. Contractor, its contracted providers, and its subcontractors shall not have a prohibited type of relationship by employing or contracting with providers or other individuals and entities excluded from participation in federal health care programs (as defined 42 United States Code [U.S.C.] § 1320a-7b(f)) pursuant to 42 U.S.C. sections 1320a-7, 1320a-7a, 1320c-5, and 1395u(j)(2). (42 C.F.R. §§ 438.214(d)(1), 438.610(b).)

3. Contractor, its contracted providers, and its subcontractors shall not have the types of relationships prohibited by this subsection E.3 with an excluded, debarred, or suspended individual, provider, or entity.
 - i. A director, officer, agent, managing employee, or partner of Contractor. (42 U.S.C. § 1320a-7(b)(8)(A)(ii); 42 C.F.R. § 438.610(c)(1).)
 - ii. A subcontractor of Contractor, as governed by 42 C.F.R. section 438.230. (42 C.F.R. § 438.610(c)(2).)
 - iii. A person with beneficial ownership of five percent or more of Contractor's equity. (42 C.F.R. § 438.610(c)(3).)
 - iv. A network provider or person with an employment, consulting, or other arrangement with Contractor for the provision of items and services that are significant and material to Contractor's obligations under this Agreement. (42 C.F.R. § 438.610(c)(4).)
4. Contractor, its contracted providers, and its subcontractors shall not employ or contract with, directly or indirectly, individuals or entities described in subsections E.1 and E.2 for the furnishing of health care, utilization review, medical social work, administrative services, management, or provision of medical services (or the establishment of policies or provision of operational support for such services). (42 C.F.R. § 438.808(b)(3).)
5. Contractor, its contracted providers, and its subcontractors shall not contract directly or indirectly with an individual convicted of crimes described in section 1128(b)(8)(B) of the Social Security Act. (42 C.F.R. § 438.808(b)(2).)
6. Contractor shall provide to County written disclosure of any prohibited affiliation identified by Contractor, its contracted providers, or its subcontractors. (42 C.F.R. § 438.608(c)(1).)

F. Disclosures.

1. **Disclosures of 5% or More Ownership Interest.** Contractor shall provide to County written disclosure of information on ownership and control of Contractor, its contracted providers, and its subcontractors (hereafter Disclosing Entity) as described in 42 C.F.R. section 455.104 and this subsection F.1 of this Section 6 (Additional State Contract Compliance Requirements). Contractor shall provide disclosures to County on a form provided by County upon submitting the provider application, before entering into a provider agreement with County, before renewing a provider agreement with County, annually and upon request

during the re-validation of enrollment process under 42 C.F.R. section 455.104, and within 35 days after any change in ownership of Disclosing Entity. The information included in the disclosures shall be current as of the time submitted. The following information must be disclosed:

- i. The name and address of any person (individual or corporation) with an ownership or control interest in Disclosing Entity. The address for corporate entities shall include, as applicable, a primary business address, every business location, and a P.O. Box address.
 - ii. Date of birth and Social Security Number (in the case of an individual).
 - iii. Other tax identification number (in the case of a corporation) with an ownership or control interest in Disclosing Entity or in any subcontractor in which Disclosing Entity has a five percent or more interest.
 - iv. Whether the person (individual or corporation) with an ownership or control interest in Disclosing Entity is related to another person with ownership or control interest in Disclosing Entity as a spouse, parent, child, or sibling; or whether the person (individual or corporation) with an ownership or control interest in any subcontractor in which Disclosing Entity has a five percent or more interest is related to another person with ownership or control interest in Disclosing Entity as a spouse, parent, child, or sibling.
 - v. The name of any other disclosing entity in which an owner of Disclosing Entity has an ownership or control interest.
 - vi. The name, address, date of birth, and Social Security Number of any managing employee of Disclosing Entity.
- 2. Disclosures Related to Business Transactions.** Contractor shall submit the following disclosures and updated disclosures related to certain business transactions to County, the California Department of Health Care Services (DHCS), or the United States Department of Health and Human Services (HHS) within 35 days upon request. The following information must be disclosed:
- i. The ownership of any subcontractor with whom Contractor has had business transactions totaling more than \$25,000 during the 12-month period ending on the date of the request; and
 - ii. Any significant business transactions between Contractor and any wholly owned supplier, or between Contractor and any subcontractor, during the 5-year period ending on the date of the request.

3. Disclosures Related to Persons Convicted of Crimes. Contractor certifies that it has submitted the following disclosures related to persons convicted of crimes to County before entering into this Agreement. Contractor shall submit the following disclosures to County or DHCS at any time upon request. The following information must be disclosed:

- i. The identity of any person who has an ownership or control interest in or is a managing employee of Contractor who has been convicted of a crime related to federal health care programs. (42 C.F.R. § 455.106(a)(1) and (2).)
- ii. The identity of any person who is an agent of Contractor who has been convicted of a crime related to federal health care programs. (42 C.F.R. § 455.106(a)(1) and (2).) For this purpose, the word “agent” has the meaning described in 42 C.F.R. section 455.101.

4. Remedies. If Contractor fails to comply with disclosure requirements, remedies available to County and DHCS include:

- i. Federal Financial Participation (FFP) is not available in expenditures for services furnished by Contractor that fail to comply with a request made by County, DHCS, or the Secretary of HHS under subsections F.1 and F.2 of this Section 6 (Additional State Contract Compliance Requirements) or under 42 C.F.R. section 420.205 (Disclosure by providers and part B suppliers of business transaction information). FFP will be denied in expenditures for services furnished during the period beginning on the day following the date the information was due to County, DHCS, or the Secretary of HHS and ending on the day before the date on which the information was supplied. (42 C.F.R. §§ 455.104(f), 455.105(c).)
- ii. Contractor shall reimburse those Medi-Cal funds received during any period for which material information was not reported, or reported falsely, to County or DHCS. (Welf. & Inst. Code, § 14043.3.)

G. Records, Audit, and Review.

1. Contractor shall maintain and preserve books and records and documents of any type whatsoever, whether physical or electronic, pertaining to Medi-Cal enrollees, Medi-Cal-related activities, or any aspect of services and activities performed, or determinations of amounts payable, under this Agreement including, but not limited to: member grievance and appeal records; the data, information, and documentation specified in (or that demonstrates compliance with) 42 C.F.R. sections 438.604, 438.606, 438.608, and 438.610; working papers;

reports; financial records and documents of account; member records; prescription files; and subcontracts (hereafter Records).

2. Contractor shall make available all of its premises, physical facilities, equipment, books, records, documents, contracts, computers, electronic systems, or any employee pertaining to Medi-Cal enrollees, Medi-Cal-related activities, or any aspect of services and activities performed, or determinations of amounts payable, under this Agreement at any time for auditing, evaluation, inspection, examination, or copying by County, the California Department of Health Care Services (DHCS), the California Department of General Services, the California State Auditor, the United States Centers for Medicare and Medicaid Services (CMS), the United States Department of Health and Human Services Office of Inspector General (HHS Inspector General), the United States Comptroller General, or other authorized federal or state agencies, or their designees (hereafter Audit). The right to Audit includes, but is not limited to, the right to Audit if County, DHCS, CMS, or the HHS Inspector General determines that there is a reasonable possibility of fraud or similar risk.
3. Both the requirement to maintain and preserve Records under subsection G.1 of this Section (Additional State Contract Compliance Requirements) and the right to Audit under subsection G.2 shall exist for 10 years from the term end date of this Agreement or as required by subsections i through iii below, whichever is later:
 - i. Applicable statute,
 - ii. Any other provision of this Agreement, or
 - iii. If any litigation, claim, negotiation, audit, or other action pertaining to Medi-Cal enrollees, Medi-Cal-related activities, or any aspect of services and activities performed, or determinations of amounts payable, under this Agreement has been started before the expiration of the 10-year period, until completion of the action and resolution of all issues which arise from it.
4. Contractor shall include subsection G (Records, Audit, and Review) of this Section (Additional State Contract Compliance Requirements) in all subcontracts to perform work under this Agreement.

H. Conflict of Interest.

1. Contractor shall comply with the conflict of interest safeguards described in 42 C.F.R. section 438.58 and the prohibitions described in section 1902(a)(4)(C) of

the Social Security Act (42 C.F.R. § 438.3(f)(2)) and the California Political Reform Act of 1974 (Gov. Code, § 81000 et seq.), Public Contract Code section 10365.5, and Government Code section 1090.

2. Contractor acknowledges and agrees that County and the California Department of Health Care Services (DHCS) intends to avoid any real or apparent conflict of interest on the part of Contractor, Contractor's subcontractor, or employees, officers, and directors of Contractor or subcontractor. Thus, County and DHCS reserve the right to determine, at their sole discretion, whether any information, assertion, or claim received from any source indicates the existence of a real or apparent conflict of interest, and if a conflict is found to exist, to require Contractor to submit additional information or a plan for resolving the conflict, subject to County and DHCS review and prior approval.
3. Conflicts of interest include:
 - i. An instance where Contractor or subcontractor, or any employee, officer, or director of Contractor or subcontractor, has an interest, financial or otherwise, whereby the use or disclosure of information obtained while performing services under this Agreement would allow for private or personal benefit or for any purpose that is contrary to the goals and objectives of this Agreement.
 - ii. An instance where Contractor's or subcontractor's employees, officers, or directors use their position for purposes that are, or give the appearance of being, motivated by a desire for private gain for themselves or others, such as those with whom they have family, business, or other ties.
4. If County is or becomes aware of a known or suspected conflict of interest, County will notify Contractor of the known or suspected conflict, and Contractor will have five working days from the date of notification to provide complete information regarding the suspected conflict to County. County may, at its discretion, authorize an extension of the timeline indicated herein in writing. If a conflict of interest is determined to exist by County or DHCS and cannot be resolved to the satisfaction of County or DHCS, the conflict may be grounds for terminating this Agreement.
5. Contractor shall include subsection H (Conflict of Interest) of this Section (Additional State Contract Compliance Requirements) in all subcontracts to perform work under this Agreement.

I. Nondiscrimination and Compliance (General Terms and Conditions 02/2025).

1. During the performance of this Agreement, Contractor and its subcontractors shall not deny this Agreement's benefits to any person on the basis of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status, nor shall they discriminate unlawfully against any employee or applicant for employment because of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status. Contractor shall ensure that the evaluation and treatment of employees and applicants for employment are free of such discrimination. Contractor and subcontractors shall comply with the provisions of the California Fair Employment and Housing Act (Gov. Code, § 12900 et seq.), the regulations promulgated thereunder (2 C.C.R. § 11000 et seq.), the provisions of article 9.5, chapter 1, part 1, division 3, title 2 of the Government Code (Gov. Code, §§ 11135–11139.5), and the regulations or standards adopted by the California Department of Health Care Services (DHCS) to implement such article. Contractor shall permit access by representatives of the California Civil Rights Department (CRD) and DHCS upon reasonable notice at any time during normal business hours, but in no case less than 24 hours' notice, to such of its books, records, accounts, and all other sources of information and its facilities as CRD or DHCS shall require to ascertain compliance with this provision. Contractor and subcontractors shall give written notice of their obligations under this provision to labor organizations with which they have a collective bargaining or other agreement. (See Cal. Code Regs., tit. 2, § 11105.)
2. Contractor shall include subsection I (Nondiscrimination and Compliance (GTC 02/2025) of this Section (Additional State Contract Compliance Requirements) in all subcontracts to perform work under the Agreement.

J. Nondiscrimination and Compliance.

1. Consistent with the requirements of applicable federal law, such as 42 C.F.R. section 438.3(d)(3) and (4), and state law, Contractor shall not engage in any unlawful discriminatory practices in the admission of members, assignments of accommodations, treatment, evaluation, employment of personnel, or in any other respect on any ground protected under federal or state law including sex, race, color, gender, gender identity, religion, marital status, national origin, ethnic group identification, ancestry, age, sexual orientation, medical condition, genetic

information, or mental or physical handicap or disability. (42 U.S.C. § 18116; 42 C.F.R. § 438.3(d)(3)–(4); 45 C.F.R. § 92.2; Gov. Code, § 11135(a); Welf. & Inst. Code, § 14727(a)(3).)

2. Contractor shall comply with the provisions of Section 504 of the Rehabilitation Act of 1973, as amended (codified at 29 U.S.C. § 794), prohibiting exclusion, denial of benefits, and discrimination against qualified individuals with a disability in any federally assisted programs or activities, and shall comply with the implementing regulations in 45 C.F.R. parts 84 and 85, as applicable.
3. Contractor shall include subsection J (Nondiscrimination and Compliance) of this Section (Additional State Contract Compliance Requirements) in all subcontracts to perform work under this Agreement.
4. Noncompliance with the nondiscrimination requirements in subsection J (Nondiscrimination and Compliance) of this Section 6 (Additional State Contract Compliance Requirements) shall constitute grounds for County or the California Department of Health Care Services to withhold payments under this Agreement.

K. Subcontract Requirements.

1. Contractor is hereby advised of its obligations pursuant to the following numbered provisions of Integrated Intergovernmental Agreement, Exhibit D (Special Terms and Conditions): Sections 1 Federal Equal Employment Opportunity Requirements; 2 Travel and Per Diem Reimbursement; 3 Procurement Rules; 4 Equipment Ownership/Inventory/Disposition; 5 Subcontract Requirements; 6 Income Restrictions; 7 Audit and Record Retention; 8 Site Inspection; 9 Federal Contract Funds; 11 Intellectual Property Rights; 12 Air or Water Pollution Requirements; 13 Prior Approval of Training Seminars, Workshops, or Conferences; 14 Confidentiality of Information; 15 Documents, Publications, and Written Reports; 18 Human Subjects Use Requirements; 19 Debarment and Suspension Certification; 20 Smoke-Free Workplace Certification; 21 Drug Free Workplace Act of 1988; 23 Payment Withhold; 26 Officials Not to Benefit; 27 Prohibited Use of State Funds for Software; 34 Suspension or Stop Work Notification; 35 Public Communications; and 37 Compliance with Statutes and Regulations; and 38 Lobbying Restrictions and Disclosure Certification.

L. Federal Equal Employment Opportunity Requirements.

1. Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, national origin, physical or

mental handicap, disability, age or status as a disabled veteran or veteran of the Vietnam era. Contractor will take affirmative action to ensure that qualified applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, sex, national origin, physical or mental handicap, disability, age or status as a disabled veteran or veteran of the Vietnam era. Such action will include, but not be limited to the following: employment, upgrading, demotion or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and career development opportunities and selection for training, including apprenticeship. Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the federal government or the California Department of Health Care Services (DHCS), setting forth the provisions of the Equal Opportunity clause, section 503 of the Rehabilitation Act of 1973 and the affirmative action clause required by the Vietnam Era Veterans' Readjustment Assistance Act of 1974 (38 U.S.C. § 4212). Such notices will state Contractor's obligation under the law to take affirmative action to employ and advance in employment qualified applicants without discrimination based on their race, color, religion, sex, national origin physical or mental handicap, disability, age or status as a disabled veteran or veteran of the Vietnam era and the rights of applicants and employees.

- 2.** Contractor will, in all solicitations or advancements for employees placed by or on behalf of Contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, national origin physical or mental handicap, disability, age or status as a disabled veteran or veteran of the Vietnam era.
- 3.** Contractor will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding a notice, to be provided by the federal government or the State, advising the labor union or workers' representative of the Contractor's commitments under the provisions herein and will post copies of the notice in conspicuous places available to employees and applicants for employment.
- 4.** Contractor will comply with all provisions of and furnish all information and reports required by section 503 of the Rehabilitation Act of 1973, as amended, the Vietnam Era Veterans' Readjustment Assistance Act of 1974 (38 U.S.C. § 4212) and of Federal Executive Order No. 11246, as amended, including by Executive Order No. 11375, "Amending Executive Order 11246 Relating to Equal

Employment Opportunity,” and as supplemented by the regulation at 41 C.F.R. part 60, “Office of the Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor,” and of the rules, regulations, and relevant orders of the Secretary of Labor.

5. Contractor will furnish all information and reports required by Federal Executive Order No. 11246, as amended, including by Executive Order 11375, “Amending Executive Order 11246 Relating to Equal Employment Opportunity,” and as supplemented by the regulation at 41 C.F.R. part 60, “Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor,” and the Rehabilitation Act of 1973, and by the rules, regulations, and orders of the United States Secretary of Labor, or pursuant thereto, and will permit access to its books, records, and accounts by the State and its designated representatives and the U.S. Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.
6. In the event of Contractor's noncompliance with the requirements of the provisions herein or with any federal rules, regulations, or orders which are referenced herein, this Agreement may be canceled, terminated, or suspended in whole or in part, and Contractor may be declared ineligible for further federal and state contracts in accordance with procedures authorized in Federal Executive Order No. 11246, as amended, and such other sanctions may be imposed and remedies invoked as provided in Federal Executive Order No. 11246, as amended, including by Executive Order 11375, “Amending Executive Order 11246 Relating to Equal Employment Opportunity,” and as supplemented by regulation at 41 C.F.R. part 60, “Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor,” or by rule, regulation, or order of the U.S. Secretary of Labor, or as otherwise provided by law.
7. Contractor will include subsection L (Federal Equal Employment Opportunity Requirements) of this Section (Additional State Contract Compliance Requirements) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to Federal Executive Order No. 11246, as amended, including by Executive Order 11375, “Amending Executive Order 11246 Relating to Equal Employment Opportunity,” and as supplemented by the regulation at 41 C.F.R. part 60, “Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor,” or section 503 of the Rehabilitation Act of 1973 (38 U.S.C. § 4212) or of

the Vietnam Era Veteran's Readjustment Assistance Act so that such provisions will be binding upon each subcontractor or vendor. Contractor will take such action with respect to any subcontract or purchase order as the Director of the Office of Federal Contract Compliance Programs or DHCS may direct as a means of enforcing such provisions including sanctions for noncompliance provided, however, that in the event Contractor becomes involved in, or is threatened with litigation by a subcontractor or vendor as a result of such direction by DHCS, Contractor may request in writing to DHCS, who, in turn, may request the United States to enter into such litigation to protect the interests of the State and of the United States.

M. Debarment and Suspension Certification.

1. Contractor agrees to comply with applicable federal suspension and debarment regulations including, but not limited to, 2 C.F.R. part 180 and 2 C.F.R. part 376.
2. Contractor certifies to the best of its knowledge and belief that it and its principals:
 - i. Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any federal department or agency;
 - ii. Have not within a three-year period preceding this Agreement been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) violation of federal or state antitrust statutes, or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, receiving stolen property, making false claims, obstruction of justice, or the commission of any other offense indicating a lack of business integrity or business honesty that seriously affects its business honesty;
 - iii. Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offenses enumerated in subsection 2.ii, subsection L (Debarment and Suspension Certification) of this Section (Additional State Contract Compliance Requirements);
 - iv. Have not within a three-year period preceding this Agreement had one or more public transactions (federal, state, or local) terminated for cause or default; and

- v. Have not within a three-year period preceding this Agreement engaged in any of the violations listed under 2 C.F.R. part 180, subpart C, as supplemented by 2 C.F.R. part 376.
3. Contractor shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under federal regulations (i.e., 48 C.F.R. part 9, subpart 9.4), debarred, suspended, declared ineligible, or voluntarily excluded from participation in such transaction unless authorized by the California Department of Health Care Services (DHCS).
4. The terms and definitions herein have the meanings set out in 2 C.F.R. part 180, as supplemented by 2 C.F.R. part 376.
5. Contractor will include subsection M (Debarment and Suspension Certification) of this Section (Additional State Contract Compliance Requirements) in all lower tier covered transactions and in all solicitations for lower tier covered transactions.
6. If Contractor knowingly violates this certification, in addition to other remedies available to the federal government, County or DHCS may terminate this Agreement for cause or default.

N. Uniform Administrative Requirements, Cost Principles, And Audit Requirements For Federal Awards.

1. Contractor shall comply with the requirements of 2 Code of Federal Regulations (C.F.R.) parts 200 and 300 and 45 Code of Federal Regulations part 75, which are incorporated herein by reference.
2. Contractor shall include these requirements in all subcontracts to perform work under this Agreement.

O. Mandatory Disclosures.

1. Contractor must promptly disclose whenever, in connection with this Agreement (including any activities or subcontracts thereunder), it has credible evidence of the commission of a violation of federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in title 18 of the United States Code (U.S.C.) or a violation of the civil False Claims Act (31 U.S.C. §§ 3729–3733). The disclosure must be made in writing to County, DHCS, the United States Centers for Medicare and Medicaid Services, and the United States Department of Health and Human Services Office of Inspector General. Contractor is also required to report matters related to County, state, or federal agency's integrity and

performance in accordance with Appendix XII of 2 Code of Federal Regulations part 200. Failure to make required disclosures can result in any of the remedies described in 2 Code of Federal Regulations section 200.339 Remedies for noncompliance. (See also 2 C.F.R. part 180, 31 U.S.C. § 3321, and 41 U.S.C. § 2313.)

2. Contractor shall include these requirements in all subcontracts to perform work under this Agreement.
3. Contractor shall also comply with the disclosure provisions set forth below in Section S (Byrd Anti-Lobbying Amendment) and this EXHIBIT AA General Provisions to this Agreement.

P. Prohibition On Certain Telecommunications And Video Surveillance Services Or Equipment.

1. Contractor is prohibited from obligating or expending loan or grant funds to:
 - i. Procure or obtain covered telecommunications equipment or services;
 - ii. Extend or renew a contract to procure or obtain covered telecommunications equipment or services; or
 - iii. Enter into a contract (or extend or renew a contract) to procure or obtain covered telecommunications equipment or services.
2. As described in section 889 of Public Law 115-232 “covered telecommunications equipment or services” means any of the following:
 - i. Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
 - ii. For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
 - iii. Telecommunications or video surveillance services provided by such entities or using such equipment; or
 - iv. Telecommunications or video surveillance equipment or services produced or provided by an entity that the United States Secretary of Defense, in

consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

3. For the purposes of this section, “covered telecommunications equipment or services” also include systems that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.
4. In implementing the prohibition under section 889 of Public Law 115-232, heads of executive agencies administering loan, grant, or subsidy programs must prioritize available funding and technical support to assist affected businesses, institutions, and organizations as is reasonably necessary for those affected entities to transition from covered telecommunications equipment or services, to procure replacement equipment or services, and to ensure that communications service to users and customers is sustained.
5. Contractor certifies that it will comply with the prohibition on covered telecommunications equipment and services in this section. Contractor and its subcontractors are not required to certify that funds will not be expended on covered telecommunications equipment or services beyond the certification provided upon accepting grant funding and those provided upon submitting payment requests and financial reports.
6. For additional information, see section 889 of Public Law 115-232 and 2 Code of Federal Regulations section 200.471.
7. Contractor shall include these requirements in all subcontracts to perform work under this Agreement.

Q. Domestic Preferences For Procurements.

1. Contractor should, to the greatest extent practicable and consistent with law, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including, but not limited to, iron, aluminum, steel, cement, and other manufactured products).
2. For purposes of this section:
 - i. “Produced in the United States” means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States.

- ii. “Manufactured products” means items and construction materials composed in whole or in part of nonferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.
3. Contractor shall include these requirements in all subcontracts to perform work under this Agreement.

R. Procurement Of Recovered Materials.

1. Contractor shall comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act of 1976 as amended, 42 United States Code section 6962. The requirements of section 6002 include procuring only items designated in guidelines of the United States Environmental Protection Agency (EPA) at 40 Code of Federal Regulations part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds \$10,000 or the value of the quantity acquired during the preceding fiscal year exceeded \$10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.
2. Contractor should, to the greatest extent practicable and consistent with law, purchase, acquire, or use products and services that can be reused, refurbished, or recycled; contain recycled content, are biobased, or are energy and water efficient; and are sustainable. This may include purchasing compostable items and other products and services that reduce the use of single-use plastic products. See Executive Order 14057, section 101, Policy.
3. Contractor shall include these requirements in all subcontracts to perform work under this Agreement.

S. Byrd Anti-Lobbying Amendment. (Applicable to federally funded agreements in excess of \$100,000.)

1. Certification and Disclosure Requirements.

- i. Contractor must file a certification (in the form set forth in EXHIBIT AA, Attachment 1, consisting of one page, entitled “Certification Regarding Lobbying”) that Contractor has not made and will not make any payment

prohibited by subsection 2 (Prohibition) of this Section (Byrd Anti-Lobbying Amendment).

- ii. Contractor must file a disclosure (in the form set forth in EXHIBIT AA, Attachment 2, entitled “Standard Form-LLL ‘Disclosure of Lobbying Activities’”) if Contractor has made or has agreed to make any payment using non-appropriated funds (to include profits from any covered federal action) in connection with a contract or grant or any extension or amendment of that contract or grant which would be prohibited under subsection 2 (Prohibition) of this Section (Byrd Anti-Lobbying Amendment) if paid for with appropriated funds.
 - iii. Contractor must file a disclosure form at the end of each calendar quarter in which there occurs any event that requires disclosure or that materially affect the accuracy of the information contained in any disclosure form previously filed by Contractor under subsection 1.ii. of this Section (Byrd Anti-Lobbying Amendment). An event that materially affects the accuracy of the information reported includes:
 - a. A cumulative increase of \$25,000 or more in the amount paid or expected to be paid for influencing or attempting to influence a covered federal action;
 - b. A change in the person(s) or individual(s) influencing or attempting to influence a covered federal action; or
 - c. A change in the officer(s), employee(s), or member(s) contacted for the purpose of influencing or attempting to influence a covered federal action.
 - iv. Contractor shall require all lower tier subcontractors to certify and disclose to the next tier above.
 - v. All disclosure forms shall be forwarded from tier to tier until received by County.
- 2. Prohibition.** Section 1352 of title 31 of the United States Code provides in part that no appropriated funds may be expended by the recipient of a federal contract or agreement, grant, loan, or cooperative agreement to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with any of the following

covered federal actions: the awarding of any federal contract or agreement, the making of any federal grant, the making of any federal loan, entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract or agreement, grant, loan, or cooperative agreement.

3. Contractor shall include these requirements in all lower tier subcontracts exceeding \$100,000 to perform work under this Agreement.

T. Clean Air Act. (Applicable to federally funded agreements in excess of \$150,000.)

1. Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act, as amended, 42 United States Code section 7401 et seq.
2. Contractor agrees to report each violation to the California Environmental Protection Agency (CalEPA) and understands and agrees that CalEPA will, in turn, report each violation as required to assure notification to County, the federal agency which provided funds in support of this Agreement, and the appropriate Environmental Protection Agency Regional Office.
3. Contractor shall include these requirements in all subcontracts exceeding \$150,000 to perform work under this Agreement.

U. Federal Water Pollution Control Act. (Applicable to federally funded agreements in excess of \$150,000.)

1. Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 United States Code section 1251 et seq.
2. Contractor agrees to report each violation to CalEPA and understands and agrees that CalEPA will, in turn, report each violation as required to assure notification to County, the federal agency which provided funds in support of this Agreement, and the appropriate Environmental Protection Agency Regional Office.
3. Contractor shall include these requirements in all subcontracts exceeding \$150,000 to perform work under this Agreement.

EXHIBIT AA – AA1
ATTACHMENT 1 &2

CERTIFICATION REGARDING
LOBBYING

ATTACHMENT 1
STATE OF CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES
CERTIFICATION REGARDING LOBBYING

The recipient certifies, to the best of his or her knowledge and belief, that:

1. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the making, awarding or entering into of this Federal contract, Federal grant, or cooperative agreement, and the extension, continuation, renewal, amendment, or modification of this Federal contract, grant, or cooperative agreement.
2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency of the United States Government, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, or cooperative agreement, the undersigned must complete and submit Standard Form LLL, "Disclosure of Lobbying Activities" (Attachment 2) in accordance with its instructions.
3. The recipient must require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontractors, subgrants, and contracts under grants and cooperative agreements) of \$100,000 or more, and that all subrecipients must certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S.C., any person who fails to file the required certification will be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

By signing or otherwise accepting the Agreement, the recipient certifies and files this Attachment 1. **CERTIFICATION REGARDING LOBBYING**, as required by Section 1352, Title 31, U.S.C., unless the conditions stated in paragraph 2 above exist. In such case, the awardee/contractor must complete and sign Attachment 2.

Alcor Solutions

Ziying Tan

Name of Contractor

DocuSigned by:
Printed Name of Person Signing for Contractor
Ziying Tan

Contract / Grant Number
6/10/2026

Signature of Person Signing for Contractor
Principal

Date

Title

After execution by or on behalf of Contractor, please return to:

Santa Barbara County Department of Behavioral Wellness Contracts Division
Attn: Contracts Manager
429 N. San Antonio Rd.
Santa Barbara, CA 93110

County reserves the right to notify the contractor in writing of an alternate submission address.

**ATTACHMENT 2
CERTIFICATION REGARDING LOBBYING**

Approved by OMB (0348-0046)
Complete this form to disclose lobbying activities pursuant to 31 U.S.C. 1352
(See reverse for public burden disclosure)

1. Type of Federal Action:		2. Status of Federal Action:		3. Report Type:	
<input type="checkbox"/> a. contract <input type="checkbox"/> b. grant <input type="checkbox"/> c. cooperative agreement <input type="checkbox"/> d. loan <input type="checkbox"/> e. loan guarantee <input type="checkbox"/> f. loan insurance		<input type="checkbox"/> a. bid/offer/application <input type="checkbox"/> b. initial award <input type="checkbox"/> c. post-award		<input type="checkbox"/> a. initial filing <input type="checkbox"/> b. material change For Material Change Only: Year _____ quarter _____ date of last report _____.	
4. Name and Address of Reporting Entity:			5. If Reporting Entity in No. 4 is Subawardee, Enter Name and Address of Prime:		
<input type="checkbox"/> Prime <input type="checkbox"/> Subawardee Tier, if known:			Congressional District, If known:		
Congressional District, If known:			Congressional District, If known:		
6. Federal Department/Agency			7. Federal Program Name/Description:		
			CDFA Number, if applicable:		
8. Federal Action Number, if known:			9. Award Amount, if known:		
10.a. Name and Address of Lobbying Registrant <i>(If individual, last name, first name, MI):</i>			b. Individuals Performing Services (including address if different from 10a. (Last name, First name, MI):		
11. Information requested through this form is authorized by title 31 U.S.C. section 1352. This disclosure of lobbying activities is a material representation of fact upon which reliance was placed by the tier above when this transaction was made or entered into. This disclosure is required pursuant to 31 U.S.C. 1352. This information will be available for public inspection. Any person that fails to file the required disclosure shall be subject to a not more than \$100,000 for each such failure.					
Signature:					
Print Name:					
Title:					
Telephone Number:					
Date:					
Federal Use Only			Authorized for Local Reproduction Standard Form-LLL (Rev. 7-97)		

INSTRUCTIONS FOR COMPLETION OF SF-LLL, DISCLOSURE OF LOBBYING ACTIVITIES

This disclosure form shall be completed by the reporting entity, whether subawardee or prime Federal recipient, at the initiation or receipt of a covered Federal action, or a material change to a previous filing, pursuant to title 31 U.S.C. section 1352. The filing of a form is required for each payment or agreement to make payment to any lobbying entity for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with a covered Federal action. Complete all items that apply for both the initial filing and material change report. Refer to the implementing guidance published by the Office of Management and Budget for additional information.

1. Identify the type of covered Federal action for which lobbying activity is and/or has been secured to influence the outcome of a covered Federal action.
2. Identify the status of the covered Federal action.
3. Identify the appropriate classification of this report. If this is a follow up report caused by a material change to the information previously reported, enter the year and quarter in which the change occurred. Enter the date of the last previously submitted report by this reporting entity for this covered Federal action.
4. Enter the full name, address, city, State and zip code of the reporting entity. Include Congressional District, if known. Check the appropriate classification of the reporting entity that designates if it is, or expects to be, a prime or subaward recipient. Identify the tier of the subawardee, e.g., the first subawardee of the prime is the 1st tier. Subawards include but are not limited to subcontracts, subgrants and contract awards under grant.
5. If the organization filing the report in item 4 checks "Subawardee," then enter the full name, address, city, State and zip code of the prime Federal recipient. Include Congressional District, if known.
6. Enter the name of the Federal agency making the award or loan commitment. Include at least one organizational level below agency name, if known. For example, Department of Transportation, United States Coast Guard.
7. Enter the Federal program name or description for the covered Federal action (item 1). If known, enter the full Catalog of Federal Domestic Assistance (CFDA) number for grants, cooperative agreements, loans, and loan commitments.
8. Enter the most appropriate Federal identifying number available for the Federal action identified in item 1 (e.g., Request for Proposal (RFP) number; Invitation for Bid (IFB) number; grant announcement number; the contract, grant, or loan award number; the application/proposal control number assigned by the Federal agency). Include prefixes, e.g., "RFP-DE-90-001".
9. For a covered Federal action where there has been an award or loan commitment by the Federal agency, enter the Federal amount of the award/loan commitment for the prime entity identified in item 4 or 5.

- a.** (a) Enter the full name, address, city, State and zip code of the lobbying registrant under the Lobbying Disclosure Act of 1995 engaged by the reporting entity identified in item 4 to influence the covered Federal action.
 - b.** (b) Enter the full names of the individual(s) performing services, and include full address if different from 10 (a). Enter Last Name, First Name, and Middle Initial (MI).
- 10.** The certifying official shall sign and date the form, print his/her name, title, and telephone number.

According to the Paperwork Reduction Act, as amended, no persons are required to respond to a collection of information unless it displays a valid OMB Control Number. The valid OMB control number for this information collection is OMB No. 0348-0046. Public reporting burden for this collection of information is estimated to average 10 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Office of Management and Budget, Paperwork Reduction Project (0348-0046), Washington, DC 20503.

EXHIBIT AA-1
GENERAL PROVISIONS

BEHAVIORAL HEALTH SERVICES ACT
SERVICES (BHSA)

EXHIBIT AA-1
GENERAL PROVISIONS
DEPARTMENT OF HEALTH CARE SERVICES
STATE PERFORMANCE REQUIREMENTS
BEHAVIORAL HEALTH SERVICES ACT (BHSA)

This Agreement shall be governed by and construed in accordance with all laws and regulations and policies and procedures governing the California Department of Health Care Services (hereafter referred to as DHCS) State Performance Agreement (Agreement No. 26-60060) which administers the Behavioral Health Services Act (BHSA), Lanterman- Petris-Short (LPS) Act, Projects for Assistance in Transition from Homelessness (PATH), Community Mental Health Services Block Grant (MHBG), Substance Abuse Treatment and Prevention Block Grant (SABG), and Crisis Counseling Assistance and Training Program (CCP) programs and oversees county provision of community mental health services pursuant to the Bronzan- McCorquodale Act.

Any BHSA program services operated under this Agreement to Medi-Cal members residing in Santa Barbara County or county of responsibility who meet the applicable access criteria, included as Exhibit A-1, unless separately and specially set forth in this General Provision or scope of work specific to each program.

County of Responsibility is defined as “the county of responsibility shall be the county whose county department is responsible for determining the initial and continuing Medi-Cal eligibility for a person or family. The appropriate county of responsibility shall be determined in accordance with the California Code Title 22 section 50120.”

1. PERFORMANCE.

- A.** Contractor must meet certain conditions and requirements to receive funding for these programs and services, as set forth in this County Performance Contract 26-60060 (hereafter referred to as the Contract or Agreement), as required by Welfare and Institutions Code (W&I) sections 5650(a), 5651, and 5897. Contractor agrees to comply with all of the conditions and requirements described herein.
- B.** Contractor must implement the BHSA consistent with this Contract (which is executed pursuant to W&I section 5897), applicable law and regulations, the BHSA County Policy Manual (hereafter referred to as the BHSA Policy Manual), and other applicable DHCS guidance. <https://policy-manual.mes.dhcs.ca.gov/behavioral-health-services-act-county-policy-manual/LIVE/>.
- C.** The defined terms enumerated in the BHSA Policy Manual apply to this Contract, except as otherwise provided.

- D. To the extent there is a conflict between the terms of this Contract and any federal or state statute or regulation or DHCS guidance issued pursuant to W&I section 5963.05 (or other applicable bulletin authority), Contractor must comply with the statute, regulation, or guidance, and the conflicting Contract provision will no longer be in effect.
 - E. There a requirement provided or referenced herein has an effective date that differs from the effective date of this Contract, Contractor is required to comply with the requirement as of its applicable effective date.
 - F. All terms and conditions set forth in the BHSA Policy Manual are hereby incorporated by reference and made a part of this Contract as if fully set forth herein.
 - G. Contactor must submit all deliverables required in this Contract in the schedule, form, and manner specified by County.
 - H. (Reserved)
 - I. (Reserved)
2. **GENERAL REQUIRMENTS.** Contract shall adhere to W&I section 5651(b) incorporated into this Contract. Contractor must:
- A. Comply with the expenditure requirements of W&I section 17608.05;
 - B. (Reserved)
 - C. (Reserved)
 - D. Comply with all provisions and requirements in law pertaining to patient rights;
 - E. (Reserved)
 - F. (Reserved)
 - G. Comply with all applicable laws and regulations for all services delivered, including all laws, regulations, and guidelines of the Behavioral Health Services Act.
3. **AMERICANS WITH DISABILITIES ACT.** County agrees to ensure that deliverables developed and produced, pursuant to this Agreement must comply with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973 as amended (29 United States Code (USC) § 794d), the Americans with Disabilities Act of 1990 (42 USC § 12101 *et seq.*), and the implementing regulations, including 36 Code of Federal Regulations (CFR) Part 1194 and 28 CFR Part 36, as applicable. In 1998, Congress amended the Rehabilitation Act of 1973 to require Federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities. California GC section 7405 codifies

section 508 of the Rehabilitation Act of 1973 and its implementing regulations requiring accessibility of electronic and information technology.

4. **EXECUTIVE ORDER N-6-22 – RUSSIA SANCTIONS.** On March 4, 2022, Governor Gavin Newsom issued Executive Order N-6-22 (the EO) regarding Economic Sanctions against Russia and Russian entities and individuals. “Economic Sanctions” refers to sanctions imposed by the U.S. government in response to Russia’s actions in Ukraine, as well as any sanctions imposed under State law. The EO directs state agencies to terminate contracts with, and to refrain from entering any new contracts with, individuals or entities that are determined to be a target of Economic Sanctions. Accordingly, should the State determine County is a target of Economic Sanctions or is conducting prohibited transactions with sanctioned individuals or entities, that will be grounds for termination of this Contract. The State must provide County advance written notice of such termination, allowing County at least 30 calendar days to provide a written response. Termination will be at the sole discretion of the State.
5. **MEDI-CAL VERIFICATION AND ENROLLMENT. (Reserved).**
6. **ELIGIBLE AND PRIORITY POPULATIONS. (Reserved)**
7. **REPORTING, DATA SUBMISSION, AND DATA SHARING REQUIREMENTS. (Reserved)**
8. **SPECIAL TERMS AND CONDITIONS.**
 - A. **Audit and Record Retention.** Contractor(s) shall maintain records, including books, documents, and other evidence, accounting procedures and practices, sufficient to properly support all direct and indirect costs of whatever nature claimed to have been incurred in the performance of this Agreement, including any matching costs and expenses. The forgoing constitutes “records” for the purpose of this provision.
 - B. **(Reserved)**
9. **GENERAL TERMS AND CONDITIONS (GTC 02/0205).**
 - A. Contractor shall adhere to the General terms and conditions herein referenced and includes: 1 Approval; 2 Amendments; 3 Assignment; 4 Audit; 5 Indemnification; 6 Disputes; 7 Termination for Cause; 8 Independent Contractor; 9 Recycling Certification; 10 Non-discrimination; 11 Certification Clauses; 12 Timeliness; 13 Compensation; 14 Governing Law; 15 Antitrust Claims; 16 Child Support Compliance Act; 17 Unenforceable Provision; 18 Priority Hiring; 19 Small Business Participation and DVBE Participation Reporting Requirements; 20 Loss Leader; and 21 Generative AI Disclosure Obligations.

B. Termination for Convenience. This provision replaces and supersedes only Provision 10(b) Termination for Convenience in Exhibit D. Note: Provision 10(a) Termination for Cause in Exhibit D remains in force as is.

1. This agreement may be terminated, in whole or in part, without cause, and without penalty, by either party by giving 30 calendar days advance written notice to the other party. Such notification must state the effective date of termination or cancellation and include any final performance and/or payment/invoicing instructions/requirements. Upon receipt of a notice of termination or cancellation from DHCS, Contractor must take immediate steps to stop performance and to cancel or reduce subsequent contract costs.
2. In the event of termination, in whole or in part, under this paragraph, the State may require the Contractor to transfer title, or in the case of licensed software, license, and deliver to the State any completed deliverables, partially completed deliverables, and any other materials related to the terminated portion of the Contract including but not limited to, computer programs, data files, user and operations manuals, system and program documentation, training programs related to the operation and maintenance of the system, and all information necessary for the reimbursement of any outstanding Medicaid claims.
3. The Contractor will be entitled to compensation upon submission of an invoice and proper proof of claim for the services and products satisfactorily rendered, subject to all payment provisions of the Agreement. Payment is limited to expenses necessarily incurred pursuant to this Agreement up to the date of termination.

10. SUBSTANCE USE PREVENTION, TREATMENT AND RECOVERY SERVICES BLOCK GRANT (SUBG). (Reserved)

EXHIBIT B(S)
FINANCIAL PROVISIONS
NON-DIRECT SERVICES

**EXHIBIT B
FINANCIAL PROVISIONS**

(Applicable to programs described in Exhibit A-1)

PERIODIC COMPENSATION (WITH ATTACHED EXHIBIT B-1 – SCHEDULE OF RATES)
--

1. **CONTRACT MAXIMUM VALUE.** For services to be rendered under this contract, Contractor shall be paid at the rate specified in the Schedule of Rates (Exhibit B-1), with a Maximum Contract Amount not to exceed \$540,000, inclusive of \$180,000 per fiscal year. Notwithstanding any other provision of this Agreement, in no event shall County pay Contractor more than this maximum contract amount for Contractor’s performance hereunder without a properly executed amendment.
2. **PAYMENT FOR SERVICES.** Payment for services and/or reimbursement of costs shall be made upon Contractor’s satisfactory performance, based upon the scope and methodology contained in EXHIBIT A-1. Payment for services shall be based upon the expenses and hourly rates for personnel, as defined in EXHIBIT B-1. Invoices submitted for payment that are based upon EXHIBIT B-1 must contain sufficient detail and provide supporting documentation to enable an audit of the charges. Invoice shall be paid within 30 days from receipt.
3. **PROPER INVOICE.** Contractor shall submit invoices by e-mail. A County’s representative shall evaluate the quality of the service performed, and if found to be satisfactory, shall initiate payment processing.
4. The invoice must show the Purchase Agreement number, the services performed or detailed statement of purchases with receipts, and the rate and authorization form, if applicable.
5. **INVOICE SUBMISSION.**

Email at ap@sbcbswell.org and should e-mail fail, invoices can be mailed to:

Accounts Payable
429 North San Antonio Road
Santa Barbara, CA 93110

6. **CORRECTION OF WORK.** County’s failure to discover or object to any unsatisfactory work or billings prior to payment will not constitute a waiver of County’s right to require Contractor to correct such work or billings or seek any other legal remedy.

**EXHIBIT B-1 MHS
SCHEDULE OF RATES AND CONTRACT MAXIMUM**

(Applicable to program(s) described in ExhibitA-1)

<u>Type of Service</u>	<u>Billing Increment</u>	<u>Monthly Minimum</u>	<u>Monthly Maximum</u>	<u>Total Contract Maximum</u>
IT Consultant Services ServiceNow Managed Service Provider (MSP)	Monthly	\$7,135.42	\$8,750.00	\$105,000
Time and Materials* (Additional Services as needed/as requested by Department)	\$125/hour or based on project implementation fees	N/A	N/A	\$75,000
FY 26-27 Total Contract Maximum Not to Exceed				\$180,000
FY 27-28 Total Contract Maximum Not to Exceed				\$180,000
FY 28-29 Total Contract Maximum Not to Exceed				\$180,000
FY 26-29 Total Contract Maximum Not to Exceed				\$540,000

* Alcor will provide Time and Material resources for as needed technical support for AccessFlow, ITSM, Asset Management, and Contracts and other scope of Services with Department written approval. Time and Materials resources will be billed at the rate specified in Exhibit B-1 (Schedule of Rates) or based on specific project requirements. Additional hours or scope of work must have written approval by the Director of the Department of Behavioral Wellness or designee, without altering the total maximum contract amount.

All reasonable travel, meals, and living expenses for all Alcor personnel who travel in support of the Project shall be billable at cost and all such expenses shall be borne by Department. Alcor consultants will follow Department travel policy.

EXHIBIT C

STANDARD

INDEMNIFICATION

AND

INSURANCE PROVISIONS

EXHIBIT C
INDEMNIFICATION AND INSURANCE REQUIREMENTS

INDEMNIFICATION

CONTRACTOR agrees to indemnify, defend (with counsel reasonably approved by COUNTY) and hold harmless COUNTY and its officers, officials, employees, agents and volunteers from and against any and all claims, actions, losses, damages, judgments and/or liabilities arising out of this Agreement from any cause whatsoever, including the acts, errors or omissions of any person or entity and for any costs or expenses (including but not limited to attorneys' fees) incurred by COUNTY on account of any claim except where such indemnification is prohibited by law. CONTRACTOR'S indemnification obligation applies to COUNTY'S active as well as passive negligence but does not apply to COUNTY'S sole negligence or willful misconduct.

NOTIFICATION OF ACCIDENTS AND SURVIVAL OF INDEMNIFICATION PROVISIONS

CONTRACTOR shall notify COUNTY immediately in the event of any accident or injury arising out of or in connection with this Agreement. The indemnification provisions in this Agreement shall survive any expiration or termination of this Agreement.

INSURANCE

CONTRACTOR shall procure and maintain for the duration of this Agreement insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work hereunder and the results of that work by the CONTRACTOR, its agents, representatives, employees or subcontractors.

1. MINIMUM SCOPE OF INSURANCE

Coverage shall be at least as broad as:

- A. Commercial General Liability (CGL):** Insurance Services Office (ISO) Form CG 00 01 covering CGL on an "occurrence" basis, including products-completed operations, personal & advertising injury, with limits no less than \$1,000,000 per occurrence and \$2,000,000 in the aggregate.
- B. Automobile Liability:** Insurance Services Office Form Number CA 0001 covering, Code 1 (any auto), or if CONTRACTOR has no owned autos, Code 8 (hired) and 9 (non-owned), with limit no less than \$1,000,000 per accident for bodily injury and property damage.
- C. Workers' Compensation:** Insurance as required by the State of California, with Statutory Limits, and Employer's Liability Insurance with limit of no less than

\$1,000,000 per accident for bodily injury or disease. (Not required if CONTRACTOR provides written verification that it has no employees)

- D. Professional Liability (Errors and Omissions):** Insurance appropriate to the CONTRACTOR'S profession, with limit of no less than \$1,000,000 per occurrence or claim, \$2,000,000 aggregate.
- E. Cyber Liability Insurance:** Cyber Liability Insurance, with limits not less than \$2,000,000 per occurrence or claim, \$2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the CONTRACTOR in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs, regulatory fines and penalties as well as credit monitoring expenses.

If the CONTRACTOR maintains higher limits than the minimums shown above, the COUNTY requires and shall be entitled to coverage for the higher limits maintained by the CONTRACTOR. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to the COUNTY.

2. Other Insurance Provisions

The insurance policies are to contain, or be endorsed to contain, the following provisions:

- A. Additional Insured** – COUNTY, its officers, officials, employees, agents and volunteers are to be covered as additional insureds on the CGL policy with respect to liability arising out of work or operations performed by or on behalf of the CONTRACTOR including materials, parts, or equipment furnished in connection with such work or operations. General liability coverage can be provided in the form of an endorsement to the CONTRACTOR'S insurance at least as broad as ISO Form CG 20 10 11 85 or if not available, through the addition of both CG 20 10 and CG 20 37 if a later edition is used).
- B. Primary Coverage** – For any claims related to this Agreement, the CONTRACTOR's insurance coverage shall be primary insurance as respects the COUNTY, its officers, officials, employees, agents and volunteers. Any insurance or self-insurance maintained by the COUNTY, its officers, officials, employees, agents or volunteers shall be excess of the CONTRACTOR'S insurance and shall not contribute with it.

- C. Notice of Cancellation** – Each insurance policy required above shall provide that coverage shall not be canceled, except with notice to the COUNTY.
- D. Waiver of Subrogation Rights** – CONTRACTOR hereby grants to COUNTY a waiver of any right to subrogation which any insurer of said CONTRACTOR may acquire against the COUNTY by virtue of the payment of any loss under such insurance. CONTRACTOR agrees to obtain any endorsement that may be necessary to effect this waiver of subrogation, but this provision applies regardless of whether or not the COUNTY has received a waiver of subrogation endorsement from the insurer.
- E. Deductibles and Self-Insured Retention** – Any deductibles or self-insured retentions must be declared to and approved by the COUNTY. The COUNTY may require the CONTRACTOR to purchase coverage with a lower deductible or retention or provide proof of ability to pay losses and related investigations, claim administration, and defense expenses within the retention.
- F. Acceptability of Insurers** – Unless otherwise approved by Risk Management, insurance shall be written by insurers authorized to do business in the State of California and with a minimum A.M. Best’s Insurance Guide rating of “A- VII.”
- G. Verification of Coverage** – CONTRACTOR shall furnish the COUNTY with proof of insurance, original certificates and amendatory endorsements as required by this Agreement. The proof of insurance, certificates and endorsements are to be received and approved by the COUNTY before work commences. However, failure to obtain the required documents prior to the work beginning shall not waive the CONTRACTOR’S obligation to provide them. The CONTRACTOR shall furnish evidence of renewal of coverage throughout the term of the Agreement. The COUNTY reserves the right to require complete, certified copies of all required insurance policies, including endorsements required by these specifications, at any time.
- H. Failure to Procure Coverage** – In the event that any policy of insurance required under this Agreement does not comply with the requirements, is not procured, or is canceled and not replaced, COUNTY has the right but not the obligation or duty to terminate the Agreement. Maintenance of required insurance coverage is a material element of the Agreement and failure to maintain or renew such coverage or to provide evidence of renewal may be treated by COUNTY as a material breach of contract.
- I. Subcontractors** – CONTRACTOR shall require and verify that all subcontractors maintain insurance meeting all the requirements stated herein, and CONTRACTOR shall ensure that COUNTY is an additional insured on insurance required from subcontractors.

J. Claims Made Policies – If any of the required policies provide coverage on a claims-made basis:

1. The Retroactive Date must be shown and must be before the date of the contract or the beginning of contract work.
2. Insurance must be maintained and evidence of insurance must be provided for at least five (5) years after completion of contract work.
3. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a Retroactive Date prior to the contract effective date, the CONTRACTOR must purchase “extended reporting” coverage for a minimum of five (5) years after completion of contract work.

K. Special Risks or Circumstances – COUNTY reserves the right to modify these requirements, including limits, based on the nature of the risk, prior experience, insurer, coverage, or other special circumstances.

Any change requiring additional types of insurance coverage or higher coverage limits must be made by amendment to this Agreement. CONTRACTOR agrees to execute any such amendment within thirty (30) days of receipt.

Any failure, actual or alleged, on the part of COUNTY to monitor or enforce compliance with any of the insurance and indemnification requirements will not be deemed as a waiver of any rights on the part of COUNTY.

EXHIBIT D
HIPAA BUSINESS ASSOCIATE
AGREEMENT (BAA)

EXHIBIT BAA
HIPAA BUSINESS ASSOCIATE AGREEMENT
(VERSION 9.25.24)

This Business Associate Agreement supplements and is made a part of the Agreement for Services of Independent Contractor between the County of Santa Barbara ("County" or "Covered Entity") and Alcor Solutions, Inc. ("Contractor" or "Business Associate").

The County of Santa Barbara 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, as amended ("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 Agreement for Services of Independent Contractor, 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 ("PHI"), as defined by the HIPAA Rules. 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 (collectively, "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" is also 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 Alcor Solutions, Inc.

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 of Santa Barbara.

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 others 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 includes, 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; or (iii) transmitted or maintained in any other form or medium.

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. §§ 164.502 (b), 164.514(d).

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 to de-identify the information in accordance with 45 C.F.R. 164.514(a)–(c) 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 Except as otherwise provided in this Business Associate Agreement, 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 as permitted under applicable law.

2.6 Except as otherwise provided in this Business Associate Agreement, 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 (i) prior written 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 (ii) a prior written agreement from the recipient requiring the recipient to notify Business Associate of any instances of which the recipient is aware in which the confidentiality of the Protected Health Information has been breached in accordance with the breach notification requirements of this Business Associate Agreement.

2.7 Except as otherwise limited in this Business Associate Agreement, Business Associate may Use Protected Health Information to provide Data Aggregation services relating to Covered Entity's Health Care Operations if such Data Aggregation services are necessary in order to provide Services.

3. PROHIBITED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION.

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

3.2 Business Associate shall not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164, or the California Confidentiality Laws if done by Covered Entity, except for the specific Uses and Disclosures set forth in Sections 2.5, 2.6, and 2.7.

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

3.4 Business Associate shall not directly or indirectly receive remuneration in exchange for any Protected Health Information of an Individual without Covered Entity's prior written approval and notice from Covered Entity that it has obtained from the Individual, in accordance with 45 C.F.R. § 164.508, a valid authorization that specifies whether the Protected Health Information can be further exchanged for remuneration by Business Associate. The foregoing shall not apply to Covered Entity's payments to Business Associate for Services delivered by Business Associate to Covered Entity.

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

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

5.2.1 Business Associate shall make an immediate telephonic report upon discovery of the non-permitted Use or Disclosure of Protected Health Information, Security Incident or Breach of Unsecured Protected Health Information to County number: 1-805-884-6855 (Privacy Line) that minimally includes:

- (a) A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident, or Breach and the date of discovery of the non-permitted Use or Disclosure, Security Incident, or Breach, if known;
- (b) The number of Individuals whose Protected Health Information is involved;
- (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 Chief Privacy/Safety Officer at:

Chief Privacy Officer: Daniel Mendoza
Department: Santa Barbara County Department of Behavioral Wellness
Address: 300 N. San Antonio Road
Santa Barbara, CA 93110
Email: dmendoza@sbcbswell.org; and
BWellPrivacy@sbcbswell.org

that includes, to the extent possible:

- (a) A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident, or Breach and the date of discovery of the non-permitted Use or Disclosure, Security Incident, or Breach, if known;
- (b) The number of Individuals whose Protected Health Information is involved;
- (c) A description of the specific type of Protected Health Information involved in the non-permitted Use or Disclosure, Security Incident, or Breach (such as whether full name, social security number, date of birth,

home address, account number, diagnosis, disability code or other types of information were involved);

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

(e) Any other information necessary to conduct an assessment of whether notification to the Individual(s) under 45 C.F.R. § 164.404 is required and any additional information reasonably requested by Covered Entity for purposes of investigating the Breach;

(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.

5.4 Business Associate's notification of non-permitted Use or Disclosure of Protected Health Information, Security Incident, or Breach of Unsecured Protected Health

Information under this Section 5 shall comply in all respects with each applicable provision of Section 13400 of Subtitle D (Privacy) of American Recovery and Reinvestment Act of 2009 (“ARRA”), the HIPAA Rules, and related guidance issued by the Secretary or the delegate of the Secretary from time to 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 the Chief Privacy Officer as listed in Section 5.2.2 above.

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 20.4.

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, and Business Associate shall thereafter provide or deny access accordingly.

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.

7.4 Business Associate agrees that when requesting, using, or disclosing Protected Health Information in accordance with 45 C.F.R. § 164.502(b)(1) that such request, use, or disclosure shall be to the minimum extent necessary to accomplish the intended purpose of such request, use, or disclosure, as interpreted under related guidance issued by the Secretary from time to time.

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, and Business Associate shall thereafter make any amendments accordingly. Business Associate agrees to take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.526.

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 thirty (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.

10.3 Business Associate agrees to comply with the "Prohibition on Sale of Electronic Health Records or Protected Health Information," as provided in Section 13405(d) of Subtitle D (Privacy) of the ARRA, and the "Conditions on Certain Contacts as Part of Health Care Operations," as provided in Section 13406 of Subtitle D (Privacy) of ARRA and related guidance issued by the Secretary from time to time.

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 or that would otherwise cause a Breach of Unsecured PHI.

13. BREACH NOTIFICATION TO INDIVIDUALS AND OTHER REQUIRED PARTIES.

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 or a Security Incident in violation of this Business Associate Agreement, provide breach notification to the Individual, the media (as defined under the Health Information Technology for Economic and Clinical Health Act of 2009 (the "HITECH Act"), the Secretary, and/or any other required parties in a manner that permits Covered Entity to comply with its obligations under HIPAA, the HITECH Act, ARRA, and the HIPAA Rules including 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 to each Individual 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.

13.1.3 The notification provided by Business Associate to the media, the Secretary, and/or any other required parties shall be subject to review and approved by Covered Entity.

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. COMPLIANCE WITH SECURITY RULE.

14.1 Business Associate shall comply with the HIPAA Security Rule, which shall mean the Standards for Security of Electronic Protected Health Information at 45 C.F.R. Part 160 and Subparts A and C of Part 164, as amended by ARRA and the HITECH Act.

14.2 In accordance with the Security Rule, Business Associate agrees to:

(a) Implement the administrative safeguards set forth at 45 C.F.R. § 164.308, the physical safeguards set forth at 45 C.F.R. § 164.310, the technical safeguards set forth at 45 C.F.R. § 164.312, and the policies and procedures set forth at 45 C.F.R. § 164.316, to reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity as required by the Security Rule. Business Associate acknowledges that the foregoing safeguards, policies, and procedures requirements shall apply to Business Associate in the same manner that such requirements apply to Covered Entity.

(b) Require that any agent, including a Subcontractor, to whom it provides such Protected Health Information agrees to implement reasonable and appropriate safeguards to protect the Protected Health Information; and

(c) Report to the Covered Entity any Security Incident of which it becomes aware.

15. DHCS REQUIREMENTS.

15.1 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.

16. INDEMNIFICATION.

16.1 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.

16.2 Section 16.1 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.

16.3 Section 16.1 is not intended by the parties to limit in any way any rights that Covered Entity may have to additional remedies 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 or under applicable law for any acts or omissions of Business Associate or its agents or Subcontractors.

17. OBLIGATIONS OF COVERED ENTITY.

17.1 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.

17.2 Covered Entity shall not request Business Associate to Use or Disclose Protected Health Information in any manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 or the California Confidentiality Laws if done by Covered Entity, except to the extent that Business Associate may Use or Disclose Protected Health Information as provided in Sections 2.3, 2.5, 2.6, and 2.7.

18. TERM.

18.1 Unless sooner terminated as set forth in Section 19 , 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.

18.2 Notwithstanding Section 18.1 , Business Associate's obligations under Sections 9, 11, 16, and 20 shall survive the termination or expiration of this Business Associate Agreement.

19. TERMINATION FOR CAUSE.

19.1 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 Covered Entity determines that Business Associate has violated a material term of this Business Associate Agreement, and Business Associate has not cured the breach or ended the violation within the time specified by Covered Entity, which shall be reasonable given the nature of the breach and/or violation, Covered Entity may terminate this Business Associate Agreement.

19.2 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 Covered Entity determines that Business Associate has violated a material term of this Business Associate Agreement, and cure is not feasible, Covered Entity may terminate this Business Associate Agreement immediately.

20. DISPOSITION OF PROTECTED HEALTH INFORMATION UPON TERMINATION OR EXPIRATION.

20.1 Except as provided in Section 20.3, upon termination for any reason or expiration of this Business Associate Agreement, Business Associate shall return to Covered Entity, or, if agreed to by Covered entity, shall destroy as provided for in Section 20.2, 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. The Protected Health Information shall be returned in a format that is reasonably expected to preserve its accessibility and usability. Business Associate shall retain no copies of the Protected Health Information.

20.2 Destruction for purposes of Section 20.2 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.

20.3 Notwithstanding Section 20.1, 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.

20.3.1 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.

20.3.2 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.

20.4 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 20.2 .

21. AUDIT, INSPECTION, AND EXAMINATION.

21.1 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 19 .

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

21.3 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.

21.4 That Covered Entity inspects, fails to inspect, or has the right to inspect as provided for in Section 21.1, 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.

21.5 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.

21.6 Section 21.1 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.

21.7 Business Associate shall notify Covered Entity within ten (10) days of learning that Business Associate has become the subject of an audit, compliance review, or complaint investigation by the Office for Civil Rights.

22. MISCELLANEOUS PROVISIONS.

22.1 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. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of Protected Health Information.

22.2 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.

22.3 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.

22.4 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.

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

22.6 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. Any provision of this Business Associate Agreement that differs from those required by the HIPAA Rules, but is nonetheless permitted by the HIPAA Rules, shall be adhered to as stated in this Business Associate Agreement.

22.7 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 Privacy Rule, the Security Rule, HIPAA, ARRA, the HITECH Act, the Consolidated Appropriations Act, 2021 (CAA-21), the HIPAA Rules, and any other privacy laws governing Protected Health Information, including the California Confidentiality Laws.

22.8 Entire Agreement. This Business Associate Agreement constitutes the entire agreement between the parties related to the subject matter of this Business Associate Agreement, except to the extent that 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 imposes more stringent requirements related to the Use and protection of Protected Health Information upon Business Associate. This Business Associate Agreement supersedes all prior negotiations, discussions, representations, or proposals, whether oral or written. This Business Associate Agreement may not be modified unless done so in writing and signed by a duly authorized representative of both parties. If any provision of this Business Associate Agreement, or part thereof, is found to be invalid, the remaining provisions shall remain in effect.

22.9 Successors and Assigns and Non-Assignment. This Business Associate Agreement will be binding on the successors and assigns of the Covered Entity and the Business Associate. However, Business Associate shall not assign, transfer, or subcontract this Business Associate Agreement or any of its rights or obligations under the Business Associate Agreement without the prior written consent of Covered Entity. Any attempted

assignment, transfer, or subcontract in violation of this provision shall be null and void and without legal effect and shall constitute grounds for termination.

22.10 California Law. Except to the extent preempted by federal law, this Business Associate Agreement shall be governed by and construed in accordance with the laws of the state of California.

22.11 Data Ownership. Business Associate acknowledges that Business Associate has no ownership rights with respect to the Protected Information.

22.12 Business Associate's Insurance. Business Associate represents and warrants that it purchases commercial insurance to cover its exposure for any claims, damages or losses arising as a result of a breach of the terms of this BAA.

22.13 Breach Pattern or Practice by Covered Entity. Pursuant to 42 U.S.C. Section 17934(b), if the Business Associate knows of a pattern of activity or practice of the Covered Entity that constitutes a material breach or violation of the Covered Entity's obligations under the Agreement or this BAA or other arrangement, the Business Associate must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, the Business Associate must terminate the Agreement or other arrangement if feasible, or if termination is not feasible, report the problem to the Secretary. Business Associate shall provide written notice to Covered Entity of any pattern of activity or practice of the Covered Entity that Business Associate believes constitutes a material breach or violation of the Covered Entity's obligations under the Agreement or this BAA or other arrangement within five (5) days of discovery and shall meet with Covered Entity to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.

22.14 Compliance with HIPAA Workforce Training. As set forth in section 164.530 of 45 CFR Business Associate is expected to adhere to the Health Insurance Portability and Accountability Act (HIPAA) regulations to the extent necessary to comply with Covered Entity's legal obligations and to develop and maintain comprehensive consumer confidentiality policies and procedures, provide annual training of all affected staff regarding those policies and procedures including Security and Privacy safeguards, and demonstrate reasonable effort to secure written and/or electronic data to document the provision of such training and agrees to make available to the Covered Entity upon request. The parties should anticipate that this agreement will be modified as necessary for full compliance with HIPAA.

22.15 Certification.

To the extent that Covered Entity determines that such examination is necessary to comply with Covered Entity's legal obligations pursuant to HIPAA relating to certification

of its security practices, Covered Entity or its authorized agents or contractors, may, at Covered Entity's expense, examine Business Associate's facilities, systems, procedures and records as may be necessary for such agents or contractors to certify to Covered Entity the extent to which Business Associate's security safeguards comply with HIPAA, the HITECH Act, the HIPAA Regulations or this BAA.

22.16 Assistance in Litigation of Administrative Proceedings.

Business Associate shall make itself, and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under the Agreement or this BAA, available to Covered Entity, at no cost to Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against Covered Entity, its directors, officers or employees based upon a claimed violation of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where Business Associate or its subcontractor, employee or agent is named adverse party.

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 section 7920.000 et seq.) 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 section 7920.000 et seq.) 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 Personal Information, Sensitive Information, or Confidential Information ("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 underlying

Agreement, Contract, Master Agreement, Work Order, or Purchase Order or other service arrangement, with or without payment (“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 the 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 PSI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DHCS PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

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

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

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

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

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

7. **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 Agreement and this Exhibit, or potential loss of confidential data affecting the 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, 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 Data Privacy webpage: <https://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.aspx>

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

- i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
- ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

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 Agreement to which it is incorporated.

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

9. **Audits and Inspections.** From time to time, DHCS may inspect the facilities, systems, books and records of the Business Associate to monitor compliance with the safeguards required

in the Information Confidentiality and Security Requirements (ICSR) exhibit. Business Associate shall promptly remedy any violation of any provision of this ICSR exhibit. The fact that DHCS inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this ICSR exhibit.

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 Agreement. The DHCS information covered under this Exhibit B consists of Personal Information (“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-1

Privacy and Security of Personal Information and Personally Identifiable Information Not Subject to HIPAA

1. Recitals.

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

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

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

b. The purpose of this Exhibit B-1 is to set forth Business Associate's privacy and security obligations with respect to PI and PII that Business Associate may create, receive, maintain, use, or disclose for or on behalf of Covered Entity pursuant to the 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 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 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 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 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 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. A-130, 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 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 Agreement or this Exhibit B-1 or potential loss of confidential data affecting the 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: <https://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.aspx>.

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

1. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
2. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

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

v. **Complete Report.** To provide a complete report of the investigation to Covered Entity and the DHCS Information Protection Unit within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report to DHCS shall be submitted on the “Privacy Incident Report” form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If DHCS requests information in addition to that listed on the “Privacy Incident Report” form, Business Associate shall make reasonable efforts to provide Covered Entity or DHCS, as applicable, with such information. If, because of the circumstances of the incident, Business Associate needs more than ten (10) working days from the discovery to submit a complete

report, the DHCS may grant a reasonable extension of time, in which case Business Associate shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. DHCS will review and approve the determination of whether a breach occurred and whether individual notifications and a corrective action plan are required.

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

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

viii. **DHCS and Covered Entity Contact Information.** To direct communications to the above referenced Covered Entity and DHCS staff, Business Associate shall initiate contact as indicated herein. Covered Entity reserves the right to make changes to the contact information below by giving written notice to the Business Associate . Said changes shall not require an amendment to this Exhibit or the 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 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 Agreement if Business Associate is found guilty of a criminal violation of HIPAA. Covered Entity may at the request of DHCS terminate the 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 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 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 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 non-compliant practice to Business Associate does not constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under the 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 164.504(e)(2)(ii)(1), and when all DHCS PI and PII is destroyed in accordance with Attachment A.

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

Attachment A

Data Security Requirements

1. Personnel Controls

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

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

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

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

2. Technical Security Controls

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

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

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

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

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

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

g. **User IDs and Password Controls.** All users must be issued a unique 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.