Attachment B – Clearwater FY 2025-28 (BC24303)

County of Santa Barbara

BOARD OF SUPERVISORS

Minute Order

July 1, 2025

Present: 5 - Supervisor Lee, Supervisor Capps, Supervisor Hartmann, Supervisor Nelson, and Supervisor Lavagnino

BEHAVIORAL WELLNESS DEPARTMENT

File Reference No. 25-00594

RE: Consider recommendations regarding an Agreement with Clearwater Security and Compliance LLC for Information Technology Services for Fiscal Years (FYs) 2025-2028, as follows:

a) Approve and authorize the Chair to execute an Agreement for Services of Independent Contractor with Clearwater Security and Compliance LLC (not a local vendor) for the provision of an annual software as a service subscription of Integrated Risk Management, a cyber risk management system, for a total maximum contract amount not to exceed $294,996.00, inclusive of $98,332.00 per FY, for the period of July 1, 2025, through June 30, 2028;

b) Delegate to the Director of the Department of Behavioral Wellness or designee the authority to suspend, delay, or interrupt the service under the Agreement for convenience per Section 20 of the Agreement, to make immaterial changes to the Agreement per section 26 of the Agreement without altering the maximum agreement amount and without requiring the Board of Supervisors' approval of an amendment of the Agreement, subject to the Board of Supervisors' ability to rescind this delegated authority at any time; and

c) Determine that the above-recommended actions are not a project that is subject to environmental review under the California Environmental Quality Act (CEQA), pursuant to CEQA Guidelines Section 15378(b)(4), finding that the actions are governmental funding mechanisms and/or fiscal activities that will not result in direct or indirect physical changes in the environment.

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

a) Approved and authorized; Chair to execute;

b) Delegated; and

c) Approved.

The motion carried by the following vote:

Ayes: 5 - Supervisor Lee, Supervisor Capps, Supervisor Hartmann, Supervisor Nelson, and Supervisor Lavagnino

Board Contract # ____

AGREEMENT FOR SERVICES OF INDEPENDENT CONTRACTOR

BETWEEN

COUNTY OF SANTA BARBARA

AND

CLEARWATER SECURITY & COMPLIANCE LLC

FOR

INFORMATION TECHNOLOGY SERVICES

TABLE OF CONTENTS

STANDARD TERMS AND CONDITIONS 3
SIGNATURE PAGE 17
EXHIBITS LIST 18
EXHIBIT A STATEMENT OF WORK 19
EXHIBIT A-1 STATEMENT OF WORK – SOFTWARE SUBSCRIPTION 20
ATTACHMENT 1 SOFTWARE SUBSCRIPTION TERMS AND CONDITIONS 21
EXHIBIT A-2 STATEMENT OF WORK – RISK ASSESSMENT PROGRAM 30
EXHIBIT B FINANCIAL PROVISIONS 34
EXHIBIT B GENERAL FINANCIAL PROVISIONS 35
EXHIBIT B-1 SCHEDULE OF RATES AND CONTRACT MAXIMUM 36
EXHIBIT C INDEMNIFICATION AND INSURANCE REQUIREMENTS 37
EXHIBIT D CERTIFICATION REGARDING LOBBYING 42
EXHIBIT BAA – HIPAA BUSINESS ASSOCIATE AGREEMENT 47

STANDARD TERMS AND CONDITIONS

AGREEMENT

FOR SERVICES OF INDEPENDENT CONTRACTOR

(Specific to this Agreement)

THIS AGREEMENT is made by and between the County of Santa Barbara (hereafter County or Department), a political subdivision of the State of California, and **Clearwater Security & Compliance LLC** (hereafter Contractor), with an address at 40 Burton Hills Boulevard, Nashville, Tennessee 37215, Suite 200, wherein Contractor agrees to provide, and County agrees to accept, the services specified herein (hereafter "Agreement").

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. Marie Lange at phone number (615) 545-1827 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:
Legal Department
Clearwater Security & Compliance LLC
40 Burton Hills Blvd., Suite 200
Nashville, Tennessee 37215
Fax: (866) 704-3394

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

3. SCOPE OF SERVICES.

Contractor agrees to provide services to County in accordance with each Statement of Work ("SOW") as an EXHIBIT A(s) (the initial SOW being labeled as Exhibit A-1, and any subsequent SOWs shall be labeled Exhibit A-2, Exhibit A-3 and so forth) attached hereto and incorporated herein by reference.

4. TERM.

Contractor shall commence performance **July 1, 2025,** and end performance upon completion, but no later than **June 30, 2028,** 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.

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 the County, in writing, any potential conflict of interest.

11. OWNERSHIP OF DOCUMENTS AND INTELLECTUAL PROPERTY.

All of Contractor's intellectual property used or generated solely by Contractor during the provision of the services and creation of any deliverables shall remain the sole property of Contractor. Contractor hereby grants to County a royalty-free (except for the payments described elsewhere herein), unlimited, perpetual, irrevocable, worldwide, non-exclusive license to use, create derivative works from, perform, display, but not to sell, transfer or sublicense, such intellectual property insofar as necessary to enable County to realize intended benefits of the services provided by Contractor hereunder (and any deliverables provided in connection therewith); provided, however, that this license does not apply to (i) any trademark, service mark, trade name, or corporate name owned or used by Contractor or any of its affiliates identified to County or (ii) any Subscription issued to or software licensed to County by Contractor under this Agreement or any separate 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.

15. INDEMNIFICATION AND INSURANCE.

Contractor agrees to the indemnification and insurance provisions as set forth in EXHIBIT C – Standard Indemnification and Insurance Provisions 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.

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 thirty (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 thirty (30) days of written notice to County of such late payment.

C. **Upon Expiration or Termination.** Upon expiration or termination of this Agreement, Contractor shall deliver to County all deliverables 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. The foregoing is cumulative and shall not affect any right or remedy which County may have in law or equity.

D. Upon expiration of any Subscription or termination of any Subscription by COUNTY, or termination of the Subscription or discontinuation of the Software by CONTRACTOR for any reason, COUNTY's access to the Software will be eliminated as of midnight on the date such termination is effective (the "Termination Date").

E. Upon any termination for cause by COUNTY, CONTRACTOR shall refund COUNTY any prepaid fees prorated for the remainder of the applicable billing period remaining upon the Termination Date.

F. It will be the responsibility of COUNTY's Account Owner to export the Data and export or print all Output from the Software prior to the Termination Date; provided, however, that if requested, CONTRACTOR will assist COUNTY with such export prior to the Termination Date. CONTRACTOR shall retain all Data and Output for a period of ninety (90) days following the Termination Date and upon COUNTY's request in writing, CONTRACTOR will grant temporary access to the terminated Subscription during such period so as to enable COUNTY to obtain a good export of its Data and Output. Promptly thereafter, CONTRACTOR shall delete the Data and Output.

20. 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.

21. 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.

22. 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.

23. 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.

24. TIME IS OF THE ESSENCE.

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

25. 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.

26. 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. No terms or conditions disclosed on CONTRACTOR's website(s) relating to the Software that vary those set out in this Agreement are applicable. 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. Requests for changes to the terms and conditions of this Agreement after April 1 of the fiscal year for which the change would be applicable shall not be considered. All requests for changes shall be in writing. Changes shall be made by an amendment pursuant to this section. Notwithstanding any other provision of this Agreement, any amendments or modifications that do not materially change the terms of this Agreement (such as changes to the Designated Representative or Contractor's address for purposes of Notice) or that are authorized by the County of Santa Barbara Board of Supervisors may be approved by the Director of the Department of Behavioral Wellness or designee in writing and shall constitute an amendment or modification of this Agreement upon execution by the Director of the Department of Behavioral Wellness or designee.

27. 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.

28. COMPLIANCE WITH LAW.

CONTRACTOR shall, at its sole cost and expense, comply with all County, State and Federal ordinances; statutes; regulations; and orders including, but not limited to, executive orders 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 ordinance or statute, shall be conclusive of that fact as between CONTRACTOR and COUNTY.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. UNIFORM ADMINISTRATIVE REQUIREMENTS, COST PRINCIPLES, AND AUDIT REQUIREMENTS FOR FEDERAL AWARDS.

A. 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.

B. Contractor shall include these requirements in all subcontracts to perform work under this Agreement.

35. MANDATORY DISCLOSURES.

A. 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.)

B. Contractor shall include these requirements in all subcontracts to perform work under this Agreement.

C. Contractor shall also comply with the disclosure provisions set forth below in Section 39 (Byrd Anti-Lobbying Amendment) and EXHIBIT A-1 General Provisions: MHS to this Agreement.

36. PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT.

A. Contractor is prohibited from obligating or expending loan or grant funds to:

1. Procure or obtain covered telecommunications equipment or services;
2. Extend or renew a contract to procure or obtain covered telecommunications equipment or services; or
3. Enter into a contract (or extend or renew a contract) to procure or obtain covered telecommunications equipment or services.

B. As described in section 889 of Public Law 115-232, "covered telecommunications equipment or services" means any of the following:

1. Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
2. 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);
3. Telecommunications or video surveillance services provided by such entities or using such equipment; or
4. 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.

C. 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.

D. 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.

E. 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.

F. For additional information, see section 889 of Public Law 115-232 and 2 Code of Federal Regulations section 200.471.

G. Contractor shall include these requirements in all subcontracts to perform work under this Agreement.

37. DOMESTIC PREFERENCES FOR PROCUREMENTS.

A. 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).

B. For purposes of this section:

1. "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.
2. "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.

C. Contractor shall include these requirements in all subcontracts to perform work under this Agreement.

38. PROCUREMENT OF RECOVERED MATERIALS.

A. 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.

B. 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.

C. Contractor shall include these requirements in all subcontracts to perform work under this Agreement.

39. BYRD ANTI-LOBBYING AMENDMENT. (Applicable to federally funded agreements in excess of $100,000.)

A. <u>Certification and Disclosure Requirements</u>.

1. Contractor must file a certification (in the form set forth in EXHIBIT D, Attachment 1, consisting of one page, entitled "Certification Regarding Lobbying") that Contractor has not made and will not make any payment prohibited by subsection B (Prohibition) of this Section (Byrd Anti-Lobbying Amendment).
2. Contractor must file a disclosure (in the form set forth in EXHIBIT D, 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 B (Prohibition) of this Section (Byrd Anti-Lobbying Amendment) if paid for with appropriated funds.
3. 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 A.2. of this Section (Byrd Anti-Lobbying Amendment). An event that materially affects the accuracy of the information reported includes:
    i. 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;
    ii. A change in the person(s) or individual(s) influencing or attempting to influence a covered federal action; or
    iii. 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.
4. Contractor shall require all lower tier subcontractors to certify and disclose to the next tier above.
5. All disclosure forms shall be forwarded from tier to tier until received by County.

B. **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.

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

40. **CLEAN AIR ACT.** (Applicable to federally funded agreements in excess of $150,000.)

A. 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.

B. 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.

C. Contractor shall include these requirements in all subcontracts exceeding $150,000 to perform work under this Agreement.

41. FEDERAL WATER POLLUTION CONTROL ACT. (Applicable to federally funded agreements in excess of $150,000.)

A. 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.

B. 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.

C. Contractor shall include these requirements in all subcontracts exceeding $150,000 to perform work under this Agreement.

42. BUSINESS ASSOCIATE.

The parties agree to and shall comply with the terms and conditions set forth in EXHIBIT BAA HIPAA Business Associate Agreement attached hereto and incorporated herein by reference.

43. SOFTWARE SUBSCRIPTIONS.

If set forth on any Statement of Work as part of the services purchased by COUNTY, CONTRACTOR shall convey to COUNTY certain non-transferrable subscription(s) to CONTRACTOR's proprietary software (the "Subscription(s)"). Details of the software being provided under such Subscription(s), the quantity of entities allotted under such Subscription(s), the terms relating to the payment of fees for the Subscription(s) and the length of period for which we shall have the right of access to the Subscription(s) shall also be set out in any Statement of Work or in Exhibits B and B-1. All Subscriptions conveyed under this Agreement shall be conveyed in accordance with the terms of the Software Subscription Agreement attached to this Contract as Attachment 1 and deemed incorporated herein. CONTRACTOR, at CONTRACTOR'S own expense, shall defend, indemnify, and hold COUNTY harmless against any claim that any 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 reasonable attorneys' fees) that may be incurred by COUNTY in connection with any such claims.

44. NON-SOLICITATION.

The parties agree that during the term of this Agreement and for one (1) year thereafter neither party will, directly or indirectly, on its own behalf or together with, through, or on behalf of any other person, partnership, corporation, trust, association, or other entity, exclusive of the other, attempt to induce any employee, subcontractor or agent of the other to terminate their employment or agency and seek or accept employment or agency elsewhere.

45. WARRANTIES; DISCLAIMERS.

Both CONTRACTOR and COUNTY represent and warrant that it has the legal power to enter into this Agreement. CONTRACTOR represents and warrants that (i) it will perform the services in a professional and workmanlike manner with due care in a manner consistent with general industry standards reasonably applicable to the provision of the Services; (ii) it will perform the Services and supply the Subscription(s) in conformance with the specifications in this Contract and the applicable Statement of Work; (iii) the Services and Subscriptions shall comply with all applicable law; (iv) it owns or otherwise has sufficient rights to the Services and Subscriptions necessary or appropriate for the performance of its obligations under this Contract, the Software Subscription Agreement and each Statement of Work; and (v) the Services and Subscriptions do not infringe any intellectual property rights of any third party.

46. FORCE MAJEURE.

Noncompliance with any obligation under this Agreement for reasons of force majeure (such as: acts, regulations or laws of any government; war or civil commotion or destruction of production facilities or materials; fire, earthquake or storm; labor disturbances; epidemic or pandemic (excluding the present COVID-19 pandemic); failure of public utilities or common carriers; and any other causes beyond the reasonable control of the party affected) shall not constitute a breach of this Agreement.

47. LEGAL DISCLAIMER.

COUNTY acknowledges and agrees that the Services provided by CONTRACTOR do not constitute legal advice. The information conveyed by CONTRACTOR to COUNTY may be based in part on current federal law and subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. Information and recommendations provided by CONTRACTOR should not be relied upon as a substitute for competent legal advice specific to COUNTY's circumstances. COUNTY SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH COUNTY'S LEGAL OR OTHER ADVISORS, AS APPROPRIATE.

THIS SECTION LEFT BLANK INTENTIONALLY

SIGNATURE PAGE FOLLOWS

SIGNATURE PAGE

Agreement for Services of Independent Contractor between the **County of Santa Barbara** and **Clearwater Security & Compliance LLC.**

IN WITNESS WHEREOF, the parties have executed this Agreement to be effective on July 1, 2025.

COUNTY OF SANTA BARBARA:

By: _____
LAURA CAPPS, CHAIR
BOARD OF SUPERVISORS

Date: 7-1-25

ATTEST:
MONA MIYASATO
COUNTY EXECUTIVE OFFICER
CLERK OF THE BOARD

By: Sheila dla Guerra
Deputy Clerk

Date: 7-1-25

CONTRACTOR:
CLEARWATER SECURITY & COMPLIANCE LLC

By: DocuSigned by: Baxter Lee
601F845DF79B45E...
Authorized Representative

Name: Baxter Lee

Title: CFO

Date: 6/18/2025

APPROVED AS TO FORM:
RACHEL VAN MULLEM
COUNTY COUNSEL

By: Signed by: Bo Bae
48A252DEFFD3466...
Deputy County Counsel

APPROVED AS TO ACCOUNTING FORM:
BETSY M. SCHAFFER, CPA
AUDITOR-CONTROLLER

By: Signed by: C. Schaffer
A99ED5BD71D04FB...
Deputy

RECOMMENDED FOR APPROVAL:
ANTONETTE NAVARRO, LMFT,
DIRECTOR
DEPARTMENT OF BEHAVIORAL
WELLNESS

By: DocuSigned by: Antonette "Toni" Navarro
2095C5A16FE1474...
Director

APPROVED AS TO FORM:
GREG MILLIGAN, ARM
RISK MANAGER

By: Signed by: Greg Milligan
05F555F00269466...
Risk Manager

EXHIBITS LIST

This Agreement includes the following Exhibits:

EXHIBIT A –STATEMENT OF WORK

EXHIBIT A-1 Statement of Work – Software Subscription

ATTACHMENT 1 – Software Subscription Terms and Conditions

EXHIBIT A-2 Statement of Work – Risk Assessment Program

EXHIBIT B – FINANCIAL PROVISIONS

EXHIBIT B General Financial Provisions

EXHIBIT B-1 Schedule of Rates and Contract Maximum

EXHIBIT C – STANDARD INDEMNIFICATION AND INSURANCE PROVISIONS

EXHIBIT C Indemnification and Insurance Requirements

EXHIBIT D – CERTIFICATION REGARDING LOBBYING

EXHIBIT BAA – HIPAA BUSINESS ASSOCIATE AGREEMENT

EXHIBIT A

STATEMENT OF WORK

EXHIBIT A-1
STATEMENT OF WORK
SOFTWARE SUBSCRIPTION

I. **PERFORMANCE.** Clearwater Security & Compliance LLC (Contractor) shall provide an annual Software Subscription of Integrated Risk Management (IRM) Analysis for Risk Analysis & Risk Response and IRM Privacy to County through which the County of Santa Barbara, Department of Behavioral Wellness staff may access online.

II. **COMPONENTS.** The Software Subscription Attachment I provided by Contractor will include the following:

A. IRM Analysis for Risk Analysis & Risk Response which:

1. Provides access to Contractor's enterprise cyber risk management system (ECRMS); and
2. Accesses, manages, monitors, and reports progress on management of all risks to the organization's information systems.
3. Analyzes, prioritizes, responds to, manages, and documents security risks to an organization's information systems. Meet Office of Civil Rights' (OCR) expectations for accurate and thorough Risk Analysis and Risk Management as mandated by 45 CFR § 164.308(a)(1)(ii)(A) and (B)

B. IRM Privacy which:

1. Assesses and documents an organization's compliance with the requirements of the HIPAA Privacy and Breach Notification Rules, identify gaps, and manage a plan to remediate gaps.
2. Identifies gaps in its compliance program; and
3. Manages a plan to remediate gaps.

ATTACHMENT 1
SOFTWARE SUBSCRIPTION TERMS AND CONDITIONS

All proprietary software developed and owned by Clearwater Security & Compliance LLC (hereafter "CONTRACTOR") and which software is subscribed to by COUNTY under purchase terms set out in this Agreement shall be provided to COUNTY under the terms and conditions set out below.

Section 1. Software.

Such software shall be collectively referred to herein as the "Software" and these Software Subscription Terms and Conditions ("SSA") describe CONTRACTOR's and COUNTY's rights and responsibilities with respect to the Software.

A. Subscriptions. CONTRACTOR grants COUNTY the limited, nontransferable (except as otherwise provided herein), non-exclusive, non-sublicensable, revocable, royalty-free (except for the payment terms described in this Agreement) right to access and use the Software (hereafter, the "Subscription(s)"), solely for and on behalf of its own internal business operations, for the specified edition, which includes (i) the number of logical assessment and/or reporting entities ("Entity(ies)") allotted to COUNTY; and (ii) certain features and functions of the Software included in the Subscription(s) based on COUNTY's payment of the Subscription Fees, as defined herein, and with respect to each Subscription, for the initial length of period ("Subscription Term") as also set out in this Agreement. Each Subscription granted hereunder is subject to the restrictions set out in this SSA. For purposes of this SSA, the verb "use" shall mean to login, access, interact with, enter data into or otherwise benefit from the Software.

B. Users and Account Owner(s). COUNTY will select and authorize at least one (1) initial primary account owner of the Software ("Account Owner(s)") on its behalf to serve on behalf of COUNTY as (i) the subject matter expert for the Software; (ii) the administrator of the Software, its settings and its users and their permissions; (iii) the trainer of other users on the functionality and use of Software; and (iv) the first point of contact to triage questions, potential issues, and/or to generally provide feedback and input to CONTRACTOR, in relation to the use of the Software by COUNTY. COUNTY will provide the name and email address for such initial Account Owner(s) and will request in writing or email that CONTRACTOR set up login credentials for such Account Owner(s). CONTRACTOR will provide and communicate such login credentials directly to the Account Owner(s) on such date COUNTY requires access to the Software. COUNTY will require all Account Owner(s) to engage in introductory training session(s) made reasonably available by CONTRACTOR as described in Section 5 below, with the objective for such Account Owner(s) to develop proficiency in use of the Software and all administrative functions. Additionally, COUNTY's Account Owner(s) may set up login credentials to access the Software for an unlimited number of individual employees and/or contractors COUNTY may authorize from time to time, including additional Account Owner(s). The Account Owner(s) and other individuals authorized by COUNTY to access the Software on its behalf will be collectively referred to as "Users." Such Users will be considered for authorization by COUNTY (i) when an Account Owner establishes login credentials and permissions to the Software for such individuals, or (ii) if an Account Owner is temporarily

unavailable, COUNTY may request CONTRACTOR to do so on its behalf by providing a written request (which may be emailed), communicating the name and email address of such individuals COUNTY authorizes and the permission parameters of such individuals. In this case, CONTRACTOR will create and maintain such User accounts based solely on COUNTY's written instructions or actions. If an Account Owner is anticipated to be unavailable, or has become unavailable, for more than thirty (30) consecutive days, and no additional Account Owner(s) has or have been designated and trained, COUNTY shall promptly designate a new Account Owner. CONTRACTOR shall provide training for up to one (1) new Account Owner per year at no cost to COUNTY. Training of Account Owner(s) in excess of the forgoing shall be subject to billing at then-current hourly rates.

COUNTY understands and acknowledges that Users authorized as an Account Owner may authorize and de-authorize Users and modify their access permissions. COUNTY also understands and acknowledges that Users will have access to make additions, deletions, or changes to COUNTY Data entered and maintained within the Software, based on permissions granted by an Account Owner. It is the responsibility of COUNTY to establish and maintain its procedures for authorizing and de-authorizing Account Owners and Users and maintaining access permissions of all Users. It is also COUNTY's responsibility to revoke Software access authorization and/or to add or change such access permissions for its Users by (i) implementation of such changes within the Software by an Account Owner; or (ii) if an Account Owner is temporarily unavailable, COUNTY may request CONTRACTOR to do so on its behalf by providing a written request (which may be emailed), setting out the name and email address of such Users and the action COUNTY authorizes.

Use of the Software requires that COUNTY or its Users provide professional and organizational contact information. CONTRACTOR may contact Users directly via email to inquire as to such Users' use of the Software as well as to make Users aware of Updates to the Software; best practices for use of the Software; education and news relating to HIPAA and/or information risk management; announcements of the availability of new resources; and other such information regarding the Software and its use. Upon receipt of an opt-out notice from any User that he/she is no longer interested in receiving such contact or information, CONTRACTOR shall promptly cease such contact with that User. Such User contact information will not be disclosed or otherwise shared with any third parties and will be used by CONTRACTOR solely for assisting COUNTY and Users with use of the Software and the Subscriptions.

A. **Right To Copy.** Only in the case of any of the policy and procedure Software, which is provided by CONTRACTOR in a one-time download format, COUNTY may make ONE additional copy of such Software solely for archival, emergency back-up, or disaster recovery purposes, provided that: (i) COUNTY shall only make one exact copy of the Software as originally delivered by CONTRACTOR, (ii) COUNTY shall ensure that the one copy contains all titles, trademarks, and copyright and restricted rights notices as in the original, and (iii) such copy shall be subject to the terms and conditions of this SSA. COUNTY understands that at no time will CONTRACTOR have access to or a copy of COUNTY's tailored version of such policy and procedure Software, once it has been downloaded and altered by COUNTY.

Section 2. Purpose and Use of Software.

The term "Software" shall mean the CONTRACTOR software, policy, and procedure templates and/or "Software as a Service" ("SaaS") services more fully-described in this Agreement, and includes without limitation the proprietary computer software, underlying algorithms, formulae and methodology, database design, associated media, printed materials, online or other User documentation provided to COUNTY, release notes, User questions and their sequence and presentation, Data (as defined below) capture forms, and the design of the Output (as defined below) resulting from the operation of the Software on the Data. The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Software is not sold. The SaaS Software and Data do not reside on COUNTY's systems. COUNTY's access to use the Software is provided solely in the form of a Subscription for which COUNTY shall pay a fee ("Subscription Fee") which shall be invoiced in the amount and frequency as more specifically described in Exhibit B and Exhibit B1 of this Agreement under which the Subscription is purchased and conveyed to COUNTY. Unless otherwise stated, CONTRACTOR's Subscription Fees as set out in this Agreement do not include any local, state, federal or foreign taxes, levies, or duties of any nature ("Taxes"). COUNTY is responsible for paying all applicable Taxes, excluding only taxes based on CONTRACTOR's business income and employees. If CONTRACTOR has the legal obligation to pay or collect Taxes for which COUNTY is responsible under this Section 2, the appropriate amount shall be invoiced to and paid by COUNTY unless COUNTY provides CONTRACTOR with a valid tax exemption certificate authorized by the appropriate taxing authority.

The Software has no requirement for creation, receipt, maintenance or transmission of, nor does it provide for the creation, receipt, maintenance or transmission of any personally identifiable information ("PII") or protected health information ("PHI"). The only information comprising the Data or Output is information concerning COUNTY's HIPAA Compliance program; its information systems used to create, receive, maintain or transmit sensitive information; and/or its information risk management program. COUNTY agrees to take reasonable steps to ensure that Authorized Users do not upload or otherwise enter any PHI or PII into the Software.

In developing the Software, CONTRACTOR has made commercially reasonable efforts to interpret and apply the provisions and requirements of the HIPAA Security Rule, the HIPAA Privacy Rule, and the HIPAA Breach Notification Rule (the "Rules") and recommended standards and best practices as set forth by the Office for Civil Rights ("OCR") under such Rules. When used as designed, the Software provides a consistent approach to the performance of certain activities required or suggested by the Rules by guiding the User through a series of questions. The Software follows a proprietary decision flow to pose such series of questions, capture the User's responses and, based on those responses, allows the Software to calculate certain proprietary compliance and/or risk management rating(s), highlight additional controls COUNTY might consider implementing and suggest tasks that COUNTY might consider completing in managing identified risks or closing compliance gaps. Although the Subscriptions to the Software shall support and promote COUNTY's compliance with the Rules, COUNTY's purchase of Subscription(s) to the Software, alone, does not assure COUNTY's compliance with the Rules.

Section 3. Legal Disclaimer.

COUNTY acknowledges and agrees that the Software provided by CONTRACTOR does not constitute legal advice. The information in the Software may be based in part on current federal

law and subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. Information and recommendations provided by CONTRACTOR should not be relied upon as a substitute for competent legal advice specific to COUNTY's circumstances. Customer should evaluate all information, opinions, and recommendations provided by Clearwater in consultation with customer's legal or other advisors, as appropriate.

Section 4. Updates to the Software.

"Update" means a subsequent release of the Software, if any, that CONTRACTOR makes generally available to subscribers of the specified edition of the Software at no additional charge. Updates will be provided at no cost to COUNTY and CONTRACTOR will provide the Software via the Subscription(s) (including all Updates), for so long as COUNTY maintains its Subscription to the specified edition, and for so long as COUNTY is current on its payment obligations; or, in the case of policy and procedure Software, for so long as CONTRACTOR continues to actively provide and maintain such Software. Updates shall include all (i) bug fixes, patches, and maintenance releases, (ii) updates to maintain consistency with Federal regulations, (iii) new point releases denoted by a change to the right of the first decimal point (e.g., v6.0 to 6.1), and (iv) new major version releases denoted by a change to the left of the first decimal point (e.g., v6.0 to 7.0) that are not Upgrades. Updates shall not include any release, option, future services, or any upgrade in features, functionality or performance of the Software which CONTRACTOR provides separately or offers only for an additional fee to all similarly situated customers subscribing to the relevant edition. All Updates to the Software shall be considered part of the Software and are subject to the terms and conditions of this SSA. "Upgrade" includes any release, option, future services, or any upgrade in features, functionality or performance of the Software which CONTRACTOR subscribes to all similarly situated customers separately or offers only for an additional fee.

Section 5. Training and Support.

Concurrent with the initial issuance of the Subscription, CONTRACTOR will schedule and provide introductory training on the functionality of and administration of the Software ("Software Training") to the Account Owner(s) designated by COUNTY, at no charge to COUNTY. Additionally, at its sole option, CONTRACTOR will proactively contact Account Owner(s) to suggest or offer ongoing Software Training when Updates occur or in response to COUNTY inquiries about the use of the Software. Software Training may take the form of live, web-based training session(s), or (if available) pre-recorded video training, at COUNTY's option. Software Training will not include the provision training on general subjects not directly related to the functionality of and administration of the Software and the Subscriptions, such as, but not limited to, general HIPAA or state privacy or security regulations and compliance, risk analysis and risk management requirements or processes, NIST publications and requirements, and the like. Such general training may be made available to COUNTY at then current hourly rates. Additionally, throughout the term of COUNTY's Subscription, CONTRACTOR will provide technical support services to Account Owners via phone and email during regular business hours, Central Time, to address issues or questions encountered by Users regarding the administration of, function of and underlying processes associated with the Software. When communicating such questions or issues, Account Owners will make reasonable efforts to provide details of the context of issues, including, but not limited to, screen shots, report examples, descriptions of the sequence of events, details of

error messages, etc. Support requests will receive an acknowledgement and status of processing such questions and issues within two business hours of receipt. CONTRACTOR will make commercially reasonable efforts to respond to questions and issues within a reasonable period. CONTRACTOR will also make commercially reasonable efforts to correct confirmed defects in the Software of which it is made aware and that are capable of being corrected, based on the severity of the defect.

Section 6. Ownership.

The Software is the sole and exclusive property of CONTRACTOR. All right, title, and interest in and to the Software, any copies thereof, including but not limited to all copyrights, trademarks, and other proprietary rights, are owned by CONTRACTOR. Without limiting the generality of the foregoing, all data entered or information provided by a User (herein "User Data" or "COUNTY Data" and collectively "Data") and the resultant data calculated or generated by the Software in the form of dashboards, charts and reports (herein "Output"), including any related COUNTY copyrights, trademarks, and other proprietary rights, remain the sole and exclusive property of COUNTY. COUNTY grants CONTRACTOR a non-exclusive, revocable, non-transferrable, non-sublicensable license to use the Data and the Output for the purposes of: (i) assisting Users and COUNTY with Support and Training on the Software; (ii) assisting Users and COUNTY to evaluate COUNTY's compliance with the Rules; and (iii) only if de-identified and in aggregate and combined with other users' de-identified data for the sole purposes of: improving the validity and capability of the Software; compiling anonymous benchmarking; and/or further evaluating the information privacy and security compliance and risk management market outlook, provided that such use will not, under any conditions, reveal the identity of COUNTY or Users. Data or Output will be maintained in confidence by CONTRACTOR in accordance with the terms of this SSA. Data and Output will be available to COUNTY, without charge, at any time during the Subscription Term. CONTRACTOR will not release, use, alter, de-identify, aggregate, sell, or perform any activity with the Data or the Output outside the scope of services of this SSA. Except for any hosting or data backup service, CONTRACTOR will not distribute Data nor the Output to any third party without first obtaining COUNTY's prior written permission. The recipient of any Data or Output from CONTRACTOR shall be obligated to comply with provisions no less stringent than those of this Section 6. CONTRACTOR will use commercially reasonable administrative, physical, and technical safeguards, to back-up and secure such Data and Output and prevent unauthorized use or disclosure of Data and Output.

Section 7. Suspension/Discontinuance of the Software and/or User Access.

CONTRACTOR reserves the right to suspend or discontinue the Software, or any portion thereof, and/or COUNTY's or its Users' use of the Software, without penalty, under certain circumstances:

(a) without prior notice or liability to COUNTY or Users, if emergency maintenance is necessary, and CONTRACTOR will promptly notify COUNTY and Account Owners of such suspension and the estimated period of time until the operation will resume; or

(b) with not less than thirty (30) days' prior written notice to COUNTY for nonpayment of Subscription Fees or other material breach of this SSA or the SOW, provided that COUNTY has been given notice of such nonpayment or breach and such breach has not been cured within such 30-day period, and provided that CONTRACTOR will promptly restore COUNTY's (or the applicable User's) access to and use of the Software after the event giving rise to the suspension has been resolved; or

(c) with not less than one hundred eighty (180) days prior written notice to COUNTY if the Software is being replaced or permanently discontinued for reasons beyond CONTRACTOR's reasonable control. In such case, CONTRACTOR will reimburse COUNTY in the amount of any unused portion of Subscription Fees paid. If the Software(s) is/are being replaced, CONTRACTOR will offer COUNTY the opportunity to subscribe to the replacement Software at the then current Subscription Fee. If COUNTY subscribes to such replacement Software, CONTRACTOR will make all commercially reasonable efforts to migrate the Data to the replacement Software.

At the time of discontinuance for any reason, CONTRACTOR will make reasonable efforts to ensure all Data will be available for COUNTY to export in CSV format and that Output can be either exported in CSV format or printed, as appropriate, as of the date of discontinuation.

Section 8. Prohibitions on Use; Other Restrictions.

COUNTY and its Users will not knowingly use the Software for any purpose that is unlawful or is prohibited by this SSA. By way of example, and not as a complete list, COUNTY and its Users will not knowingly:

(a) Alter or tamper with the Software in any way.

(b) Attempt to defeat any security measures that CONTRACTOR may take to protect the confidential and proprietary nature of the Software.

(c) Remove, obscure, conceal, or alter any marking or notice of patent, copyright, trademark, trade name, or other proprietary rights that may appear on or within the Software.

(d) Sell, lease, license, rent, loan, resell, or otherwise transfer (including, but not limited to, transferring or sharing the Software electronically from one computer to another through any communication means or over a computer network), with or without consideration, to or with any third party except as otherwise permitted hereunder.

(e) Share use of the Software with third parties through the sharing of login credentials or any other means.

(f) Make any attempt to reverse engineer, disassemble, decompile, or otherwise attempt to derive the source code, algorithms or formulae used within the Software.

(g) Modify or create derivative works based upon the Software, or any portion thereof, provided that COUNTY may tailor policy and procedure Software solely for its own use.

(h) Use the Software in any manner that could damage, disable, overburden, or impair CONTRACTOR's website or servers or networks connected to the website.

(i) Use the Software in a manner that interferes with any other party's use of the Software.

Section 9. Login Credentials.

Each User is responsible for selecting a strong password and for maintaining the confidentiality and security of his/her User ID and password. Each User is responsible for all activity occurring under User's login credentials, except if such login credentials were compromised due to an act or omission of CONTRACTOR or unauthorized third-party intervention. Each party will promptly notify the other upon becoming aware of unauthorized use of any User's login credentials.

Section 10. Access Rights.

If CONTRACTOR reasonably and in good faith believes that a User has violated the terms of this SSA, CONTRACTOR may investigate such alleged misuse of or access to the Software without prior notice to the User or COUNTY to determine whether a violation has occurred. Promptly thereafter, CONTRACTOR shall provide the results of its investigation to COUNTY for the parties to determine, in good faith, the appropriate action to be taken.

Section 11. Feedback.

In the event a User or COUNTY provides any comments, suggestions, or ideas ("Feedback") to CONTRACTOR regarding the Software or otherwise, COUNTY acknowledges and agrees that (i) at its sole option, CONTRACTOR shall have the right to retain and use such Feedback to develop or improve current or future products or services, without obligation or compensation to COUNTY or User and without COUNTY's or its Users' approval, provided that CONTRACTOR removes from the Feedback any confidential or proprietary information of COUNTY and any information that could disclose the identity of COUNTY, any User, or the creator of the Feedback; and (ii) CONTRACTOR may already have something similar to the Feedback from other COUNTYs or Users or under consideration or development.

Section 12. Disclaimer of Warranties.

CONTRACTOR represents and warrants that it has the legal power to enter into this SSA. CONTRACTOR represents and warrants that (i) it shall supply the Subscriptions in conformance with the specifications in this SSA, (ii) the Software and the Training and Support of the Software described in Section 5 of this SSA will be provided in a professional, workmanlike and timely manner with due care in a manner consistent with general industry standards reasonably applicable to the provision of such Software and support, (iii) the Subscriptions shall comply with all applicable laws, (iv) it owns and has sufficient rights to the Software necessary or appropriate for the performance of its obligations under this SSA, and (v) the Software and use thereof as contemplated by this SSA does not and will not infringe any intellectual property or other rights of any third party or violate applicable law. Clearwater represents and warrants that the software is and will remain free from viruses and malware. Except as specifically set forth in this SSA, Clearwater, to the maximum extent permitted by applicable law, expressly disclaims any and all other warranties for the software whether express, implied or statutory, including without limitation the implied warranty of merchantability and fitness for a particular purpose. Clearwater cannot ensure that access to the software will be uninterrupted and error free.

Section 13. Limitation of Liability.

To the maximum extent permitted by applicable law, except for any indemnity provided by either party to the other in this SSA or any other agreement, in no event shall either party be liable for any punitive, special, incidental, indirect, or consequential damages whatsoever, whether based in contract, tort (including without limitation negligence), or otherwise, arising out of the use of or inability to use the software, even if such party has been advised of the possibility of such damages.

If customer is dissatisfied with any portion of the software, the sole and exclusive remedy in respect of the software is to discontinue use of the software and terminate the SSA. Except for any indemnity provided by either party to the other in this SSA, in no event shall either party's liability to the other party arising out of or related to this SSA, whether in contract, tort (including without limitation negligence), or under any other theory of liability, exceed three times the amount

actually paid by and due from customer under this SSA. Because some jurisdictions do not allow the exclusion or limitation of liability, the above limitation may not apply to customer.

Section 14. Confidentiality.

"Confidential Information" means any information of any type in any form that (i) is disclosed to or observed or obtained by one party from the other party in the course of, or by virtue of, this Agreement; and (ii) either is designated as confidential or proprietary at the time of such disclosure or within a reasonable time thereafter or is of a nature that the recipient knew or reasonably should have known, under the circumstances, that would be regarded by the owner of the information as confidential or proprietary. Without limiting any other provisions of this Agreement, and whether or not otherwise meeting the criteria described herein, the Software shall be deemed conclusively to be Confidential Information of CONTRACTOR and all Data and Output shall be deemed conclusively to be Confidential Information of COUNTY.

For purposes of this Agreement, however, the term "Confidential Information" specifically shall not include any portion of the foregoing that (i) was in the recipient's possession or knowledge at the time of disclosure and that was not acquired directly or indirectly from the other party, (ii) was disclosed to the recipient by a third party not having an obligation of confidence of the information to any person or body of which the recipient knew or which, under the circumstances, the recipient reasonably should have assumed to exist, (iii) is or, other than by the act or omission of the recipient, becomes a part of the public domain not under seal by a court of competent jurisdiction, or (iv) was independently developed by the recipient without breach of any obligation owed to the disclosing party. In the event of any ambiguity as to whether information is Confidential Information, the foregoing shall be interpreted strictly and there shall be a rebuttable presumption that such information is Confidential Information. COUNTY represents and warrants to CONTRACTOR that all such Confidential Information heretofore and in the future disclosed to CONTRACTOR in connection with this Agreement has been and will be disclosed in a manner which does not violate the rights of third parties.

Except as otherwise may be permitted by this Agreement or as necessary to comply with the law including, but not limited to, the California Public Records Act and the Ralph M. Brown Act, neither party shall disclose any Confidential Information of the other party to any person without the express prior written consent of the other party; provided, however, that either party may disclose appropriate portions of Confidential Information of the other party to those of its employees, contractors, agents, service providers and professional advisors having a substantial need to know the specific information in question in connection with professional advice to be provided to the party or with such party's exercise of rights or performance of obligations under this Agreement, provided that all such persons (i) have been instructed that such Confidential Information is subject to the obligation of confidence set forth by this Agreement and (ii) are bound either by contract, employment policies, or fiduciary or professional ethical obligations to maintain such information in confidence.

Notwithstanding any other provision of this Agreement, if either party is ordered by a court, administrative agency, or other governmental body of competent jurisdiction, or is otherwise required by law to disclose Confidential Information, then such party shall immediately notify the other party of the order or rule (if not prohibited by order or law from informing the other party) by the most expeditious possible means. Clearwater acknowledges that the County is subject to the California Public Records Act and the California Brown Act.

The recipient agrees to protect the confidentiality of the Confidential Information of the other party in the same manner that it protects the confidentiality of its own proprietary and confidential information of like kind, but in no event shall either party exercise less than reasonable care in protecting the Confidential Information. If the recipient becomes aware that Confidential Information has been disclosed due to a breach in security or otherwise, it shall provide the disclosing party with notice in reasonable detail of the disclosure promptly. If the recipient discloses or uses (or threatens to disclose or use) any Confidential Information of the disclosing party in breach of this Section 14 the disclosing party shall be entitled, in addition to any other remedies available to it, to seek injunctive relief to enjoin the acts, all without the requirement of posting bond or having to prove the inadequacy of monetary damages, it being specifically acknowledged by the parties that any other available remedies are inadequate.

Both parties shall return or delete relevant Confidential Information held by it upon termination of this Agreement, subject to CONTRACTOR's obligations in Section 19 (Termination) of the Standard Terms and Conditions of this Agreement; provided, however, that it is understood that information in an intangible or electronic format cannot be immediately removed, erased or otherwise deleted from system back-ups but that such information will continue to be protected under the confidentiality requirements contained in this Agreement. Notwithstanding any other provision of this Agreement, upon termination of this Agreement, either party may retain a copy of Confidential Information to fulfill a legal or regulatory obligation, or its document retention policies and practices (including any litigation data destruction holds). The obligations and rights of this Section 14 shall survive termination of this Agreement or any Subscriptions granted hereunder.

EXHIBIT A-2
STATEMENT OF WORK
RISK ASSESSMENT PROGRAM

1. **PERFORMANCE**. Clearwater Security & Compliance LLC (Contractor) shall perform an annual Information Technology (IT) security risk assessment for three (3) consecutive years for the Department of Behavioral Wellness (County) as required by the Department of Behavioral Wellness' policy and procedure 14.001, 45 CFR Section 164.308 (a)(1)(ii)(A)[1], and the National Institute of Standards and Technology ("NIST") Special Publications ("SP") describing risk assessments, risk management and controls. Public Law 116-3213[2]. Contractor shall:

   A. Have the background, training, work experience, accreditation, licenses, and supervision necessary for the performance of services in a manner of and according to the standards observed by a practitioner of the same profession and in keeping with all pertinent Federal, State, and County laws; and

   B. Warrant that said accreditation and licensing information furnished to County is complete and accurate and agrees to notify County promptly of any changes in this information.

2. **COMPONENTS.** The security risk assessment program to be performed by Contractor will include the following:

   A. Key Program phases:
      1. Overall Program Support by a Designated Program Leader.
      2. Ongoing preparation and planning, including scheduling of site visits/reviews and discovery interviews, as applicable.
      3. Conducting on-site visits and discovery interviews.
      4. Entry of information systems into the IRM|Analysis Software, identification of components, and characterization of properties for grouping.
      5. Performance of risk determination.
      6. Analysis.
      7. Preparation and presentation of FOR Report.
      8. Remediation Planning and Support.

   B. Contractor shall provide the following deliverables:
      1. Contractor's fully populated Clearwater IRM Analysis software;
      2. Draft and final Summary FOR Report(s); and

[1] http://www.ecfr.gov/cgi-bin/text-idx?SID=f27b0e2ed3da04ecf4c9fe25c2edb8d1&mc=true&node=se45.1.164_1308&rgn=div8
[2] https://www.govinfo.gov/app/details/PLAW-116publ321/summary

3. Remediation Planning and Support results in an average of 1.5 risks per information system for high and critical risk or Program Support Deliverables related to *adoption of recognized security practices under Public Law 116-321

3. **SERVICES.** The completion of the security risk assessment each year ("Program") will enable County to meet explicit HIPAA Security Rule requirements for risk analysis as mandated by 45 CFR Section 164.308 (a)(1)(ii)(A). Performance of this risk assessment will also help County demonstrate the adoption of recognized security practices under Public Law 116-321, and identify, rate, and prioritize all risks to the specific information assets that are used to create, receive, maintain, and/or transmit its e-Patient Health Information (PHI). Contractor will utilize Clearwater IRM Analysis software and assessment process to perform the information security risk analysis. Details of the Program include:

A. Overall Program Support by a Designated Program Leader.
1. Program Leader will augment County's Cyber Risk Management ("CRM") team and provide Program oversight, guidance, and hands-on support to County's Program team.
2. Facilitate seamless performance of the Program.
3. Exercise oversight for development of the Program Plan, project plans for the execution of Services and updates.
4. Communicate Program status to County.

B. Planning and Preparation: Planning and preparation of schedule by Contractor and County staff.
1. IT Risk Assessment program is dependent upon County's Subject Matter Experts (SMEs) ability to provide the requested documentation, commit in advance to schedule, prepare for and fully engage in discovery interviews, training opportunities, and document reviews.

C. Site Visit(s): Performance of site visit and review by Contractor consultants of primary physical location of where County's information assets are managed or housed.

1. Contractor's consultants will visit County's location based on a schedule that will be mutually agreed upon by Contractor and County;
2. The County location is **315 Camino Del Remedio, Bldg. 3, Santa Barbara, CA 93110**.
3. All administrative, physical, and technical security controls used to protect relevant information will be evaluated at this site.
4. County SME(s) responsible for each in-scope information asset and the relevant security control areas will be interviewed and applicable procedures, processes, and practices will be reviewed within the scope of the discovery.
5. Follow-up interviews may also be conducted via telephone, web meetings, conference calls, and email.
6. Based on the quantity of information assets provided in the inventory developed above, it is estimated that discovery visits and interviews can be completed over

the course of two (2) to three (3) business days and will require a total of one (1) trip by two (2) consultants.

D. Information Asset Inventory: The scope of the risk analysis will include information assets used by County to create, receive, maintain, or transmit sensitive information. Contractor and County will determine the information assets to be analyzed each program year through execution of the Information Asset Inventory.

1. A detailed inventory was developed by Contractor and County regarding County's current information system environment and needs. The following **twelve (12)** assets will be analyzed each program year:

   i. Admin Workstations;
   ii. Clinicians Gateway- Krassons Technologies (EHR);
   iii. EOB Database;
   iv. Microsoft 365;
   v. Network fileshare;
   vi. Reportal database (in- house);
   vii. ServiceNow;
   viii. ShareCare Billing (Echo Group);
   ix. Smartsheet;
   x. Tableau;
   xi. RX30/Pyxis (Med Station); and
   xii. SmartCare (EHR).

E. On-going training of County staff by Contractor in the use of the IRM Analysis software during and after engagement with Contractor to operationalize the maintenance of Customer's risk analyses and ongoing information risk management program;

F. Interviews of County SMEs by Contractor and documentation reviews each Program Year;

1. Contractor relies heavily on information provided in interviews and documentation provided by County SMEs assigned to the Project.

G. Project status reports as mutually agreed upon by County and Contractor; and

H. Provision of complete documentation and reporting of the risk analysis results and risk response actions during the engagement and after.

I. Data entry, analysis, preparation, and presentation of an Executive Summary of the engagement process and results by Contractor in one comprehensive Findings, Observations, and Recommendations (FOR) Report each Program Year.

J. The findings and recommendations of the (IT) security risk assessment provided in the FOR Report presentation will set out the degree to which County's information technology

and cybersecurity practices align with recognized security practices under Public Law 116-3213.

K. Planning, preparation, the initial software training, the documentation review, the detailed data entry into the Software, analysis, and FOR Report preparation will be conducted remotely.

EXHIBIT B

FINANCIAL PROVISIONS

EXHIBIT B
PAYMENT ARRANGEMENTS

A. 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 value not to exceed **$294,996,** the value shown on the Purchase Agreement B1. Notwithstanding any other provision of this Contract, in no event shall County pay Contractor more than this Maximum Contract Amount for Contractor's performance hereunder without a properly executed amendment.

B. 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. Payment for services shall be based upon the expenses, 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.

C. Proper Invoice. Contractor shall submit to County's representative an invoice or certified claim on the County treasury for the service performed over the period specified. County's representative shall evaluate the quality of the service performed, and if found to be satisfactory, shall initiate payment processing.

a. The invoice must show the Purchase Agreement number, the services performed or detailed statement of purchases with receipts, the rate and authorization form, if applicable.

b. County's Designated Representative:

Santa Barbara County
Department of Behavioral Wellness
Attn: Accounts Payable
429 North San Antonio Road
Santa Barbara, CA 93110
ap@sbcbwell.org

D. 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
SCHEDULE OF FEES

Type of Service	Unit Reimbursement	Total Maximum Contract Value
IT Services: User Software Subscription	$26,045 per fiscal year for FY 2025-28	$78,135 FY 2025-28
IT Services: Clearwater Risk Assessment Program	$72,287 for FY 2025-28	$216,860 for FY 2025-28
Annual Contract Amount FY 2025-26		**$98,332**
Annual Contract Amount FY 2026-27		**$98,332**
Annual Contract Amount FY 2027-28		**$98,332**
Total Maximum Contract Amount FY 2025-28		***$294,996**

- License/Subscription Fees are based on the: (a) Edition selected, (b) size of the organization into which the Subscription is being deployed, as measured by the quantity of beds/components/workforce members within the organization, and (c) length of Renewal Term selected.
- ASF is invoiced yearly
- Quarterly fee will be invoiced upon execution of this Amended and Restated Agreement.
- Subsequent quarterly payments will be invoiced on the fifth (5th) day of each quarter for the remainder of the contract term.
- Any payment made with a credit card will incur an additional fee of three percent (3%) added upon payment of fees.

EXHIBIT C

STANDARD

INDEMNIFICATION

AND

INSURANCE PROVISIONS

EXHIBIT C
INDEMNIFICATION AND INSURANCE REQUIREMENTS
(For Information Technology Contracts)
(Specific to this Agreement)

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 ("Claims") arising out of this Agreement and for any costs or expenses (including but not limited to attorneys' fees) ("Costs") incurred by COUNTY on account of any (i) breach of the Agreement by CONTRACTOR resulting in the unauthorized disclosure of COUNTY's confidential information, (ii) violation of applicable law by CONTRACTOR, or (iii) gross negligence or willful misconduct of CONTRACTOR, provided in no event will CONTRACTOR be required to indemnify COUNTY to the extent any such Claims or Costs would not have arisen but for gross negligence or intentional misconduct of COUNTY or any of its officers, officials, employees, agents or volunteers.

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.

A. Minimum Scope of Insurance

Coverage shall be at least as broad as:

1. **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.
2. **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.
3. **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)**

4. **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.

5. **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.

B. Other Insurance Provisions

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

1. **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).

2. **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.

3. **Notice of Cancellation** – Each insurance policy required above shall provide that coverage shall not be canceled, except with notice to the COUNTY.

4. **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.

5. **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.
6. **Acceptability of Insurers** – Unless otherwise approved by Risk Management, insurance shall be written by insurers authorized to do business in the State of – Tennessee and with a minimum A.M. Best's Insurance Guide rating of "A- VII".
7. **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.
8. **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.
9. **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.
10. **Claims Made Policies** – If any of the required policies provide coverage on a claims-made basis:
    i. The Retroactive Date must be shown and must be before the date of the contract or the beginning of contract work.
    ii. Insurance must be maintained and evidence of insurance must be provided for at least five (5) years after completion of contract work.
    iii. 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.
11. **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; provided that if any such modification would increase the cost of the insurance CONTRACTOR is required to maintain hereunder, it may request that COUNTY reimburse CONTRACTOR in the

amount of such increased cost, and if COUNTY declines to do so, then in lieu of procuring such additional insurance CONTRACTOR may terminate this Agreement without penalty.

Any change requiring additional types of insurance coverage or higher coverage limits must be made by amendment to this Agreement.

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
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.

Clearwater Security & Compliance, LLC	Baxter Lee
Name of Contractor	Printed Name of Person Signing for Contractor
	DocuSigned by: Baxter Lee
Contract / Grant Number	Signature of Person Signing for Contractor
6/18/2025	CFO
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:
— a. contract b. grant c. cooperative agreement d. loan e. loan guarantee f. loan insurance	— a. bid/offer/application b. initial award c. post-award	a. initial filing 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:
☐Prime ☐Subawardee Tier , 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 *(If individual, last name, first name, MI)*:	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 itis, 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.

10. (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) 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).

11. 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 BAA

HIPAA BUSINESS ASSOCIATE AGREEMENT

EXHIBIT BAA -

HIPAA BUSINESS ASSOCIATE AGREEMENT

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 **CLEARWATER SECURITY & COMPLIANCE LLC** ("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 may 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 solely to the extent that Business Associate does create, receive, maintain, transmit, or access Protected Health Information on behalf of Covered Entity.

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 **CLEARWATER SECURITY & COMPLIANCE LLC**.

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 include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

1.11 "Electronic Protected Health Information" has the same meaning as the term "electronic protected health information" at 45 C.F.R. § 160.103, limited to Protected Health Information created or received by Business Associate from or on behalf of Covered Entity. For the convenience of the parties, Electronic Protected Health Information means Protected Health Information that is (i) transmitted by electronic

media; (ii) maintained in electronic media; 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 Officer at:

Chief Privacy Officer:	Jamie Huthsing, LMFT
Department:	Santa Barbara County Department of Behavioral Wellness, Quality Care Management/Access Team
Address:	300 N. San Antonio Road Santa Barbara, CA 93110
Email:	jhuthsing@sbcbwell.org and BWellPrivacy@sbcbwell.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.

5.5 Notwithstanding the foregoing, the parties agree that this Section 5.5 of the Business Associate Agreement constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of unsuccessful security incidents which are not of a type or pattern that warrant further action or represent a threat to the security of the system or any Protected Health Information contained or transmitted therein.

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), connected with Business Associate's grossly negligent acts or willful misconduct 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

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 Pl. 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 Pl. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DHCS PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

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.

b. ***Security Officer***. Business Associate shall, to the extent it has not already done so, designate a Security Officer to oversee its data security program who will be responsible for carrying out its privacy and security programs and for communicating on security matters with Covered Entity and DHCS.

Discovery and Notification of Breach. Notice to Covered Entity:

i. To notify Covered Entity and DHCS **immediately** upon the discovery of a suspected security incident that involves data provided to Covered Entity by DHCS from the Social Security Administration. This notification will be by **telephone call plus email or fax** upon the discovery of the breach. (2) To notify Covered Entity **within 24 hours by email or fax** of the discovery of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of the 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. A130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

iii. If the data obtained by Business Associate from DHCS through Covered Entity includes PII, Contractor shall also comply with the substantive privacy and security requirements in the CMPPA Agreement. Business Associate also agrees to ensure that any agents, including a subcontractor to whom it provides DHCS PII, agree to the same requirements for privacy and security safeguards for confidential data that apply to Business Associate with respect to such information.

d. **Mitigation of Harmful Effects**. To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of DHCS PI or PII by Business Associate or its subcontractors in violation of this Exhibit B-1.

e. **Business Associate's Agents and Subcontractors**. To impose the same restrictions and conditions set forth in this Exhibit B-1 on any subcontractors or other agents with whom Business Associate subcontracts any activities under the 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 two (2) business days 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	**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 noncompliant 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 1 64.504(e)(2)(ii)(1), and when all DHCS PI and PII is destroyed in accordance with Attachment A.

14. **Effect of Termination**. Upon termination or expiration of this Agreement for any reason, Business Associate shall return or destroy all DHCS PHI, PI and PII that Business Associate still maintains in any form, and shall retain no copies of such PHI, PI or PII. If return or destruction is not feasible, Business Associate shall notify Covered Entity an DHCS of the conditions that make the return or destruction infeasible, and Covered Entity, DHCS, and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI, PI or PII. Business Associate shall continue to extend the protections of this 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 Pl. 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 Pl. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DHCS PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

5. Paper Document Controls

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

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

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

d. **Removal of Data**. Only the minimum necessary DHCS PHI or PI may be removed from the premises of Business Associate except with express written permission of DHCS. DHCS PHI or PI shall not be considered "removed from the premises" if it is only being transported from one of Business Associate's locations to another of Business Associates locations.

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

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