Exhibit F
Privacy and Security Provisions

1. This Agreement has been determined to constitute a business associate relationship under the Health Insurance Portability and Accountability Act and its implementing privacy and security regulations at 45 Code of Federal Regulations, Parts 160 and 164 (collectively "HIPAA") only to the extent that Contractor performs functions or activities on behalf of the Department pursuant to this Agreement that are described in the definition of "business associate", including, but not limited to, utilization review, quality assurance, or benefit management.

2. The term "Agreement" as used in this document refers to and includes both this Privacy and Security Provisions and the contract to which this Privacy and Security Provisions is attached as an exhibit.

3. For purposes of this Agreement, the term "Business Associate" shall have the same meaning as set forth in 45 CFR section 160.103.

4. The Department of Health Care Services (DHCS) intends that Contractor may create, receive, maintain, transmit or aggregate certain information pursuant to the terms of this Agreement, some of which information may constitute Protected Health Information (PHI) and/or confidential information protected by Federal and/or state laws.

4.1 As used in this Agreement and unless otherwise stated, the term "PHI" refers to and includes both "PHI" as defined at 45 CFR section 160.103 and Personal Information (PI) as defined in the Information Practices Act at California Civil Code section 1798.3(a). PHI includes information in any form, including paper, oral, and electronic. The term PHI, as used in this exhibit, shall mean PHI accessed by Contractor in a database maintained by DHCS, received by Contractor from the Department, or acquired, or created by Contractor in connection with performing the functions, activities, and services on behalf of DHCS as specified in this Agreement.

4.2 As used in this Agreement, the term "confidential information" refers to information not otherwise defined as PHI in Section 4.1 of this Agreement, but to which state and/or federal privacy and/or security protections apply.

5. Contractor, on DHCS's behalf, provides services or arranges, performs or assists in the performance of functions or activities on behalf of DHCS, and may create, receive, maintain, transmit, aggregate, use or disclose PHI (collectively, "use or disclose PHI") in order to fulfill Contractor's obligations under this Agreement. DHCS and Contractor are each a party to this Agreement and are referred to, collectively, as the "parties."

6. The terms used in this Agreement, but not otherwise defined, shall have the same meanings as those terms in HIPAA. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

7. **Permitted Uses and Disclosures of PHI by Contractor**. Except as otherwise indicated in this Agreement, Contractor may use or disclose PHI, inclusive of de-identified data derived from such PHI, only to perform functions, activities or services specified in this Agreement on behalf of DHCS, provided that such use or disclosure would not violate HIPAA or other applicable laws if done by DHCS.

7.1 **Specific Use and Disclosure Provisions**. Except as otherwise indicated in this Agreement, Contractor may use and disclose PHI if necessary for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor. Contractor may disclose PHI for this purpose if the disclosure is required by law, or if the Contractor obtains reasonable assurances from the person to whom the information is disclosed 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 person, and the person notifies the Contractor of any instances of which it is aware that the confidentiality of the information has been breached.

Exhibit F
Privacy and Security Provisions

8. Compliance with Other Applicable Law

8.1 To the extent that other state and/or federal laws provide additional, stricter and/or more protective (collectively, more protective) privacy and/or security protections to PHI or other confidential information covered under this Agreement beyond those provided through HIPAA, Contractor agrees:

8.1.1 To comply with the more protective of the privacy and security standards set forth in applicable state or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the individuals whose information is concerned; and

8.1.2 To treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate, pursuant to Section 17 of this Agreement.

8.2 Examples of laws that provide additional and/or stricter privacy protections to certain types of PHI and/or confidential information, as defined in Section 4. of this Agreement, include, but are not limited to the Information Practices Act, California Civil Code sections 1798-1798.78, Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2, Welfare and Institutions Code section 5328, and California Health and Safety Code section 11845.5.

8.3 If Contractor is a Qualified Service Organization (QSO) as defined in 42 CFR section 2.11, Contractor agrees to be bound by and comply with subdivisions (2)(i) and (2)(ii) under the definition of QSO in 42 CFR section 2.11.

9. Additional Responsibilities of Contractor

9.1 **Nondisclosure**. Contractor shall not use or disclose PHI or other confidential information other than as permitted or required by this Agreement or as required by law.

9.2 **Safeguards and Security**.

9.2.1 Contractor shall use safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI and other confidential data and comply, where applicable, with subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by this Agreement. Such safeguards shall be based on applicable Federal Information Processing Standards (FIPS) Publication 199 protection levels.

9.2.2 Contractor shall, at a minimum, utilize a National Institute of Standards and Technology Special Publication (NIST SP) 800-53 compliant security framework when selecting and implementing its security controls and shall maintain continuous compliance with NIST SP 800-53 as it may be updated from time to time. The current version of NIST SP 800-53, Revision 5, is available online at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final; updates will be available online at https://csrc.nist.gov/publications/sp800.

9.2.3 Contractor shall employ FIPS 140-2 validated encryption of PHI at rest and in motion unless Contractor determines it is not reasonable and appropriate to do so based upon a risk assessment, and equivalent alternative measures are in place and documented as such. FIPS 140-2 validation can be determined online at https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search, with information about the Cryptographic Module Validation Program under FIPS 140-2 available online at https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-2. In addition, Contractor shall maintain, at a minimum, the most current industry standards for transmission and storage of PHI and other confidential information.

Exhibit F
Privacy and Security Provisions

9.2.4 Contractor shall apply security patches and upgrades, and keep virus software up-to-date, on all systems on which PHI and other confidential information may be used.

9.2.5 Contractor shall ensure that all members of its workforce with access to PHI and/or other confidential information sign a confidentiality statement prior to access to such data. The statement must be renewed annually.

9.2.6 Contractor shall identify the security official who is responsible for the development and implementation of the policies and procedures required by 45 CFR Part 164, Subpart C.

9.3 **Contractor's Agent.** Contractor shall ensure that any agents, subcontractors, subawardees, vendors or others (collectively, "agents") that use or disclose PHI and/or confidential information on behalf of Contractor agree to the same restrictions and conditions that apply to Contractor with respect to such PHI and/or confidential information.

10. **Mitigation of Harmful Effects**. Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of PHI and other confidential information in violation of the requirements of this Agreement.

11. **Access to PHI.** Contractor shall make PHI available in accordance with 45 CFR section 164.524.

12. **Amendment of PHI.** Contractor shall make PHI available for amendment and incorporate any amendments to protected health information in accordance with 45 CFR section 164.526.

13. **Accounting for Disclosures.** Contractor shall make available the information required to provide an accounting of disclosures in accordance with 45 CFR section 164.528.

14. **Compliance with DHCS Obligations.** To the extent Contractor is to carry out an obligation of DHCS under 45 CFR Part 164, Subpart E, comply with the requirements of the subpart that apply to DHCS in the performance of such obligation.

15. **Access to Practices, Books and Records.** Contractor shall make its internal practices, books, and records relating to the use and disclosure of PHI on behalf of DHCS available to DHCS upon reasonable request, and to the federal Secretary of Health and Human Services for purposes of determining DHCS' compliance with 45 CFR Part 164, Subpart E.

16. **Return or Destroy PHI on Termination; Survival.** At termination of this Agreement and any successor agreements, if feasible, Contractor shall return or destroy all PHI and other confidential information received from, or created or received by Contractor on behalf of, DHCS that Contractor still maintains in any form and retain no copies of such information. If return or destruction is not feasible, Contractor shall notify DHCS of the conditions that make the return or destruction infeasible, and DHCS and Contractor shall determine the terms and conditions under which Contractor may retain the PHI. If such return or destruction is not feasible, Contractor shall extend the protections of this Agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

17. **Breaches and Security Incidents.** Contractor shall implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and take the following steps:

17.1 **Notice to DHCS.**

17.1.1 Contractor shall notify DHCS **within 24 hours by email** (or by telephone if Contractor is unable to email DHCS) of the discovery of:

Exhibit F
Privacy and Security Provisions

17.1.1.1 Unsecured PHI if the PHI is reasonably believed to have been accessed or acquired by an unauthorized person;
17.1.1.2 Any suspected security incident which risks unauthorized access to PHI and/or other confidential information;
17.1.1.3 Any intrusion or unauthorized access, use or disclosure of PHI in violation of this Agreement; or
17.1.1.4 Potential loss of confidential data affecting this Agreement.

17.1.2 Notice shall be provided to the DHCS Program Contract Manager (as applicable), the DHCS Privacy Office, and the DHCS Information Security Office (collectively, “DHCS Contacts”) using the DHCS Contact Information at Section 17.6. below.

Notice shall be made using the current DHCS “Privacy Incident Reporting Form” (“PIR Form”; the initial notice of a security incident or breach that is submitted is referred to as an “Initial PIR Form”) and shall include all information known at the time the incident is reported. The form is available online at
https://www.dhcs.ca.gov/formsandpubs/laws/priv/Documents/Privacy-Incident-Report-PIR.pdf .

Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI, Contractor shall take:

17.1.2.1 Prompt action to mitigate any risks or damages involved with the security incident or breach; and

17.1.2.2 Any action pertaining to such unauthorized disclosure required by applicable Federal and State law.

17.2 **Investigation.** Contractor shall immediately investigate such security incident or confidential breach.

17.3 **Complete Report**. To provide a complete report of the investigation to the DHCS contacts within ten (10) working days of the discovery of the security incident or breach. This “Final PIR” must include any applicable additional information not included in the Initial Form. The Final PIR Form shall include an assessment of all known factors relevant to a determination of whether a breach occurred under HIPAA and other applicable federal and state laws. The report shall also include a full, detailed corrective action plan, including its implementation date and information on mitigation measures taken to halt and/or contain the improper use or disclosure. If DHCS requests information in addition to that requested through the PIR form, Contractor shall make reasonable efforts to provide DHCS with such information. A “Supplemental PIR” may be used to submit revised or additional information after the Final PIR is submitted. DHCS will review and approve or disapprove Contractor’s determination of whether a breach occurred, whether the security incident or breach is reportable to the appropriate entities, if individual notifications are required, and Contractor’s corrective action plan.

17.3.1 If Contractor does not complete a Final PIR within the ten (10) working day timeframe, Contractor shall request approval from DHCS within the ten (10) working day timeframe of a new submission timeframe for the Final PIR.

17.4 **Notification of Individuals**. If the cause of a breach is attributable to Contractor or its agents, Contractor shall notify individuals accordingly and shall pay all costs of such notifications, as well as all costs associated with the breach. The notifications shall comply with applicable federal and state law. DHCS shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.

Exhibit F
Privacy and Security Provisions

17.5 Responsibility for Reporting of Breaches to Entities Other than DHCS. If the cause of a breach of PHI is attributable to Contractor or its subcontractors, Contractor is responsible for all required reporting of the breach as required by applicable federal and state law.

17.6 DHCS Contact Information. To direct communications to the above referenced DHCS staff, the Contractor shall initiate contact as indicated here. DHCS reserves the right to make changes to the contact information below by giving written notice to Contractor. These changes shall not require an amendment to this Agreement.

DHCS Program Contract Manager	**DHCS Privacy Office**	**DHCS Information Security Office**
See the Scope of Work exhibit for Program Contract Manager information.	Privacy Office c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 Email: incidents@dhcs.ca.gov Telephone: (916) 445-4646	Information Security Office DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: incidents@dhcs.ca.gov

18. Responsibility of DHCS. DHCS agrees to not request the Contractor to use or disclose PHI in any manner that would not be permissible under HIPAA and/or other applicable federal and/or state law.

19. Audits, Inspection and Enforcement

19.1 From time to time, DHCS may inspect the facilities, systems, books and records of Contractor to monitor compliance with this Agreement. Contractor shall promptly remedy any violation of this Agreement and shall certify the same to the DHCS Privacy Officer in writing. Whether or how DHCS exercises this provision shall not in any respect relieve Contractor of its responsibility to comply with this Agreement.

19.2 If Contractor is the subject of an audit, compliance review, investigation or any proceeding that is related to the performance of its obligations pursuant to this Agreement, or is the subject of any judicial or administrative proceeding alleging a violation of HIPAA, Contractor shall promptly notify DHCS unless it is legally prohibited from doing so.

20. Termination

20.1 Termination for Cause. Upon DHCS' knowledge of a violation of this Agreement by Contractor, DHCS may in its discretion:

20.1.1 Provide an opportunity for Contractor to cure the violation and terminate this Agreement if Contractor does not do so within the time specified by DHCS; or

20.1.2 Terminate this Agreement if Contractor has violated a material term of this Agreement.

20.2 Judicial or Administrative Proceedings. DHCS may terminate this Agreement if Contractor is found to have violated HIPAA, or stipulates or consents to any such conclusion, in any judicial or administrative proceeding.

21. Miscellaneous Provisions

Exhibit F
Privacy and Security Provisions

21.1 **Disclaimer**. DHCS makes no warranty or representation that compliance by Contractor with this Agreement will satisfy Contractor's business needs or compliance obligations. Contractor is solely responsible for all decisions made by Contractor regarding the safeguarding of PHI and other confidential information.

21.2. **Amendment**.

21.2.1 Any provision of this Agreement which is in conflict with current or future applicable Federal or State laws is hereby amended to conform to the provisions of those laws. Such amendment of this Agreement shall be effective on the effective date of the laws necessitating it, and shall be binding on the parties even though such amendment may not have been reduced to writing and formally agreed upon and executed by the parties.

21.2.2 Failure by Contractor to take necessary actions required by amendments to this Agreement under Section 21.2.1 shall constitute a material violation of this Agreement.

21.3 **Assistance in Litigation or Administrative Proceedings**. Contractor shall make itself and its employees and agents 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 and/or employees based upon claimed violation of HIPAA, which involve inactions or actions by the Contractor.

21.4 **No Third-Party Beneficiaries**. Nothing in this Agreement is intended to or shall confer, upon any third person any rights or remedies whatsoever.

21.5 **Interpretation**. The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA and other applicable laws.

21.6 **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.