EXHIBIT F
PRIVACY & SECURITY REQUIREMENTS

A. Purpose of Exhibit

1. This Exhibit sets forth the privacy and security requirements that apply to all Personally Identifiable Information (PII) that Contractor obtains, maintains, transmits, uses or discloses from the California Health Benefit Exchange ("Exchange" aka Covered California) pursuant to this Agreement.

2. The parties agree to all terms and conditions of this Exhibit in order to ensure the integrity, security, and confidentiality of the information exchanged pursuant to this Agreement, and to allow disclosure and use of such information only as permitted by law and only to the extent necessary to perform functions and activities pursuant to this Agreement.

3. This Exhibit establishes requirements in accordance with applicable federal and state privacy and security laws including, but not limited to, the Information Practices Act (California Civil Code section 1798 et seq.), the federal Patient Protection and Affordable Care Act (P.L. 111-148), as amended by the federal Health Care and Education Reconciliation Act of 2010 (P.L. 111-152) (herein, the "Affordable Care Act"), and its implementing regulations at 45 C.F.R. Sections 155.260 and 155.270 (the "Exchange Privacy and Security Rules") and, where applicable, the Health Insurance Portability and Accountability Act (42 U.S.C. section 1320d-d8) and the Health Information Technology for Economic and Clinical Health Act and their implementing regulations at 45 C.F.R. Parts 160 and 164 (collectively, "HIPAA").

B. Definitions

The following definitions shall apply to this Exhibit:

1. Breach: Shall mean either: (i) the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical, or electronic; or (ii) a reasonable belief that unauthorized acquisition of PII that compromises the security, confidentiality or integrity of the PII has occurred

2. Disclosure: The release, transfer, provision of access to, or divulging in any other manner of PII outside the entity holding the information.

EXHIBIT F
PRIVACY & SECURITY REQUIREMENTS

3. Federal Tax Information or FTI: Any return or return information as defined under the Internal Revenue Service Code, 26 U.S.C. section 6103(b)(1) and (2), received from the IRS or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information. (IRS Pub. 1075, § 1.4.1)

4. Personal Information or PI: Information that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual. (California Civil Code section 1798.3)

5. Personally Identifiable Information or PII: Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (OMB M-07-16.) PII includes Federal Tax Information (FTI), Personal Information (PI) and Protected Health Information (PHI).

6. Protected Health Information or PHI: Individually Identifiable Health Information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as defined in 45 C.F.R. section 160.103.

7. Security Incident: The act of violating an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction. Adverse events such as floods, fires, electrical outages, and excessive heat are not considered incidents. (Computer Matching Agreement, Agreement No. 2013-11, p.5.)

EXHIBIT F
PRIVACY & SECURITY REQUIREMENTS

C. Applicable Laws

Contractor shall comply with any and all federal and state privacy and security laws, as well as applicable rules and regulations pertaining to the Exchange including, but not limited to, those arising under the federal Patient Protection and Affordable Care Act and its implementing regulations. To the extent a conflict arises between any laws or other requirements, Contractor agrees to comply with the applicable requirements imposing the more stringent privacy and security standards.

1. Exchange Privacy and Security Rules (45 C.F.R. section 155.260).

   a. In accessing, collecting, using or disclosing PII in performing functions for the Exchange as authorized by this Agreement, Contractor shall only use or disclose PII to the minimum extent such information is necessary to perform such functions.

   b. Contractor shall establish and implement privacy and security standards that are consistent with the principles of 45 C.F.R. section 155.260(a)(3) as set forth below in subsections (1) through (8):

      1) Individual access. Individuals shall be provided with a simple and timely means to access and obtain their PII in a readable form and format;

      2) Correction. Individuals shall be provided with a timely means to dispute the accuracy or integrity of their PII and to have erroneous information corrected or to have a dispute documented if their requests are denied;

      3) Openness and transparency. Contractor shall be open and transparent regarding its policies, procedures, and technologies that directly affect individuals and/or their PII;

      4) Individual choice. Individuals shall be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their PII;

      5) Collection, use and disclosure limitations. PII shall be created, collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately;

EXHIBIT F
PRIVACY & SECURITY REQUIREMENTS

6) Data quality and integrity. Contractor will take reasonable steps to ensure that PII is complete, accurate, and up-to-date to the extent necessary for Contractor's intended purposes and has not been altered or destroyed in an unauthorized manner;

8) Safeguards. PII will be protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure; and,

9) Accountability. Contractor will use appropriate monitoring and other means and methods to assure accountability with these principles and to report and mitigate non-adherence and breaches.

2. California Information Practices Act. Contractor shall comply with the applicable privacy and security provisions of the Information Practices Act of 1977, California Civil Code section 1798 et seq. and shall provide assistance to the Exchange as may be reasonably necessary for the Exchange to comply with these provisions (Civil Code section 1798 et seq.).

3. Health Insurance Portability and Accountability Act ("HIPAA").

a. Contractor expressly acknowledges and agrees that the Exchange is not a health care provider, a health care plan, or a health care clearinghouse. Accordingly, the parties mutually acknowledge and agree that, for purposes of this Agreement, the Exchange is not a Covered Entity as such term is specifically defined in HIPAA.

b. Contractor expressly acknowledges and agrees that where the Exchange performs a function required under applicable law pursuant to 45 C.F.R. section 155.200, it is not acting as a Business Associate of any other Covered Entity and Contractor is not acting as the Exchange's Business Associate, as such terms are specifically defined in HIPAA.

c. For certain programs related to the administration of the Medi-Cal Program, the Exchange has agreed to be the Business Associate of the Department of Health Care Services (DHCS). Therefore, to

EXHIBIT F
PRIVACY & SECURITY REQUIREMENTS

the extent that Contractor performs services related to the administration of the Medi-Cal program, contractor is the Exchange's subcontractor, and therefore, also a Business Associate as that term is specifically defined in HIPAA. Accordingly, if in performing functions pursuant to this Agreement Contractor accesses or uses PII that was provided to the Exchange by DHCS or for the purposes of the Medi-Cal program, Contractor shall comply with the applicable terms and conditions of HIPAA.

4. IRS Code section 6103 and Publication 1075. Per the Exchange Privacy and Security Rules (45 CFR 155.260 (a)(4)(iii), return information shall be kept confidential under 26 U.S. Code section 6103. As described by IRS publication 1075, conforming to the guidelines set forth in that publication meets the safeguard requirements of 26 U.S. Code section 6103(p)(4) for FTI.

5. Fingerprinting and Background Checks (CA Government Code Section 1043).

   a. All individuals including, but not limited to, employees, contractors, or subcontractors who perform services under this agreement shall agree to criminal background checks in compliance with Government Code section 1043, and its implementing regulations set forth in California Code of Regulations, Title 10, section 6456.

   b. For any insurance agent licensed by the California Department of Insurance (CDI) the Exchange may obtain a criminal history check in accordance with Government Code section 1043 from CDI.

D. Consumer Rights

1. Accounting of Disclosures

   a. Contractor shall assist the Exchange in responding to accounting requests by individuals that are made to the Exchange under the Information Practices Act (Civil Code section 1798.25-29) and if Protected Health Information is involved, pursuant to HIPAA, 45 C.F.R. section 164.528.

   b. The obligation of Contractor to provide an accounting of disclosures as set forth herein survives the expiration or termination of this Agreement with respect to accounting requests made after such expiration or termination.

EXHIBIT F
PRIVACY & SECURITY REQUIREMENTS

2. Copies of Records Requests

Regardless of whether a request is made to the Exchange or to Contractor, Contractor shall respond to the request with respect to the record Contractor and its subcontractors maintain, if any, in a manner and time frame consistent with requirements specified in the Information Practices Act (Civil Code sections 1798.30-1798.34) and if Protected Health Information is involved, with HIPAA (45 C.F.R section 164.524).

3. Requests to Amend Records

a. Contractor shall make any amendments to Personally Identifiable information in a record that the Exchange directs or agrees to, whether at the request of the Exchange or an Individual.

b. Regardless of whether a request to amend records is made to the Exchange or to Contractor, Contractor shall respond to the request with respect to the record Contractor and its subcontractors maintain in a manner and time frame consistent with requirements specified in the Information Practices Act (Civil Code section 1798.35) and if Protected Health Information is involved, with HIPAA (45 C.F.R. section 164.526).

4. Requests to Restrict Use and Disclosure of Personally Identifiable Information

a. Contractor shall reasonably comply with any requests to restrict the use and disclosure of Personally Identifiable Information.

b. If Protected Health Information is involved, Contractor shall respond to the request in a manner and time frame consistent with requirements specified in HIPAA (45 C.F.R. section 164.522).

5. Confidential Communications Request

a. Upon receipt of written notice, Contractor shall reasonably comply with any requests to utilize an alternate address, email, or telephone number when communicating with the individual.

b. If the request is denied, a written response shall be sent to the individual stating the reasons for denying the request.

EXHIBIT F
PRIVACY & SECURITY REQUIREMENTS

c. If Protected Health Information is involved, Regardless of whether a request is made to the Exchange or to Contractor, Contractor shall respond to the request in a manner and time frame consistent with requirements specified in HIPAA (45 C.F.R. section 164. 522 (b)(1)).

6. In responding to any requests from individuals, Contractor shall verify the identity of the person making the request to ensure that the person is the individual who is the subject of the PII or has authority to make requests concerning the PII before responding to the request.

7. In the event any individual submits any of these requests directly from Contractor, Contractor shall within five (5) calendar days forward such request to the Exchange.

E. <u>Security Controls and Safeguards</u>

1. At a minimum, contractor shall establish and implement operational, technical, administrative and physical safeguards that are consistent with any applicable laws to ensure

a. The confidentiality, integrity, and availability of personally identifiable information created, collected, used, and/or disclosed by the Exchange;

b. Personally identifiable information is only used by or disclosed to those authorized to receive or view it;

c. Return information, as such term is defined by section 6103(b)(2) of the Code, is kept confidential under section 6103 of the Code;

d. Personally identifiable information is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information;

e. Personally identifiable information is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law; and

f. Personally identifiable information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules.

EXHIBIT F
PRIVACY & SECURITY REQUIREMENTS

2. Encryption: Contractor shall encrypt all PII that is in motion or at rest, including but not limited to data on portable media devices, using commercially reasonable means, consistent with applicable Federal and State laws, regulations and agency guidance, including but not limited to the U.S. Department of Health and Human Services guidance specifying the technologies and methodologies that render PII unusable, unreadable, or indecipherable to unauthorized individuals for purposes of the breach notification requirements or issued by the National Institute for Standards and Technology ("NIST") concerning the protection of identifiable data such as PII. Data centers shall be encrypted or shall otherwise comply with industry data security best practices.

3. Hardware: Contractor shall ensure that any and all hardware, including but not limited to personal computers, laptops, jump-drives, smart phones or other devices upon which PII is stored is secured, password-protected and only accessible by Contractor or Contractor's agents, employees or sub-contractors in accordance with the terms of this Exhibit. Contractor shall at all times remove and permanently delete any and all PII before any such hardware is transferred or sold to a third-party or is otherwise subject to any change in ownership or control.

4. Contractor shall update these safeguards as appropriate and as requested by the Exchange.

F. <u>Policies and Procedures:</u>

1. Contractor shall implement and maintain written policies and procedures to ensure the privacy and security of PII stored, maintained, or accessed in compliance with this agreement and any applicable laws. Such policies shall address

   a. Implementation of consumer rights as required by this Exhibit;

   b. Reasonable safeguards as required by this Exhibit;

   c. Monitoring, periodically assessing, and updating security controls and related system risks to ensure the continued effectiveness of those controls;

   d. Training employees, contractors, and subcontractors.

EXHIBIT F
PRIVACY & SECURITY REQUIREMENTS

2. Upon request, Contractor shall provide the Exchange with a written policies and procedures adopted by Contractor to meet its obligations under this Section.

G. Subcontractors

1. Contractor shall be bound by and be responsible for the acts and omissions of its subcontractors, agents or vendors in the exchange of data with the Exchange. Contractor shall take reasonable steps to ensure compliance with the terms of this Agreement by its subcontractors, agents and vendors.

2. Contractor agrees to enter into written contracts with its agents and contractors (collectively, "subcontractors") that obligate Contractor's subcontractors to abide by the same privacy and security standards and obligations that Contractor has agreed to in this agreement.

3. Contractor represents and agrees that it shall only request that the Exchange transmit data to subcontractors with whom it has such agreements and only to the extent such information is necessary to carry out the purposes authorized by this Agreement.

4. Upon request, Contractor shall provide the Exchange with a copy of any written agreement or contract entered into by Contractor and its subcontractors to meet the obligations of Contractor under this Exhibit.

H. Breaches & Security Incidents

1. Contractor shall immediately report to the Exchange Privacy Officer at PrivacyOfficer@covered.ca.gov any actual or suspected Breaches or Security Incidents involving PII created or received under this Agreement. Contractor's report shall contain the following information to the extent applicable and known at that time:

   a. A brief description of what happened including the date of the incident and the date of the discovery of the incident;

   b. The names or identification numbers of the individuals whose PII has been, or is reasonably believed to have been accessed, acquired, used or disclosed

   c. A description of the types of PII that were involved in the incident, as applicable;

EXHIBIT F
PRIVACY & SECURITY REQUIREMENTS

d. Information regarding any information system intrusion and any systems potentially compromised;

e. A brief description of Contractor's investigation and mitigation plan; and

f. Any other information necessary for the Exchange to conduct an investigation and include in notifications to the individual(s) or relevant regulatory authorities under applicable privacy and security requirements.

2. Upon completion of the initial report, contractor shall immediately commence an investigation in accordance with applicable law to:

a. Determine the scope of the incident;

b. Mitigate harm that may result from the incident; and

c. Restore the security of the system to prevent any further harm or incidents.

3. Contractor shall cooperate with the Exchange in investigating the actual or suspected incident and in meeting the Exchange's obligations, if any, under applicable laws.

4. Contractor shall mitigate to the extent practicable any harmful effect of any Incident that is known or reasonably discoverable to Contractor.

5. After conducting its investigation, and within fifteen (15) calendar days, unless an extension is granted by the Exchange, Contractor shall file a complete report with the information listed above in subsection (1), if available. Contractor shall make all reasonable efforts to obtain all relevant information and shall provide an explanation if any information cannot be obtained. The complete report shall include a corrective action plan that describes the steps to be taken to prevent any future reoccurrence of the incident.

6. Contractor shall cooperate with the Exchange in developing content for any public statements and shall not give any public statements without the express written permission of the Exchange.

EXHIBIT F
PRIVACY & SECURITY REQUIREMENTS

7. If a Breach requires notifications and reporting under applicable laws, and the cause of the Breach is attributable to Contractor, its agents or subcontractors, Contractor shall:

   a. Be fully responsible for providing breach notifications and reporting as required under applicable laws;

   b. Pay any costs of such Breach notifications as well as any costs or damages associated with the incident; and

   c. Should the Exchange in its sole discretion determine that credit monitoring is an appropriate remedy, arrange for and bear the reasonable, out-of-pocket cost of providing to each such affected individual one (1) year of credit monitoring services from a nationally recognized supplier of such services.

8. If Contractor determines that an impermissible acquisition, use, or disclosure of PII does not require breach notifications or reporting, it shall document its assessment and provide such documentation to the Exchange within one week of its completion. Notwithstanding the foregoing, the Exchange reserves the right to reject Contractor's assessment and direct Contractor to treat the incident as a Breach.

I. Right to Inspect

The Exchange may inspect the facilities, systems, books, and records of Contractor to monitor compliance with this Exhibit at any time. Contractor shall promptly remedy any violation reported to it by the Exchange and shall certify the same to the Exchange Privacy Officer in writing. The fact that the Exchange inspects, fails to inspect, fails to detect violations of this Exhibit or detects but fails to notify Contractor of the violation or require remediation is not a waiver of the Exchange's rights under this Agreement and this Exhibit.

J. Indemnification

Contractor shall indemnify, hold harmless, and defend the Exchange from and against any and all costs (including mailing, labor, administrative costs, vendor charges, and any other costs the Exchange determines to be reasonable), losses, penalties, fines, and liabilities arising from or due to Contractor's failure to comply with the requirements of this Exhibit, including a breach or other non-permitted use or disclosure of PII by Contractor or its subcontractors or agents, including without limitation. Such indemnification shall be conditioned upon the Exchange giving notice of any claims to Contractor after discovery thereof. If

EXHIBIT F
PRIVACY & SECURITY REQUIREMENTS

Contractor should publish or disclose PII to others, the Exchange shall be entitled to injunctive relief or any other remedies to which it is entitled under law or equity, without posting a bond.

K. Termination of Agreement

1. If Contractor breaches its obligations under this Exhibit as determined by the Exchange, the Exchange may, at its option:

   a. Require Contractor to submit to a plan of monitoring and reporting, as the Exchange may deem necessary to maintain compliance with this Agreement;

   b. Provide Contractor with an opportunity to cure the breach; or

   c. After giving Contractor an opportunity to cure the breach, or upon breach of a material term of this Exhibit, terminate this Agreement for cause pursuant to Exhibit C.

   A failure of the Exchange to exercise any of these options shall not constitute a waiver of its rights under this section.

2. Upon completion of this Agreement, or upon termination of this Agreement, at the Exchange's direction Contractor shall either return all PII to the Exchange, or shall destroy all PII in a manner consistent with applicable State and Federal laws, regulations, and agency guidance on the destruction of PII. If return or destruction of PII is not feasible, Contractor shall explain in writing to the Exchange's Chief Privacy Officer why return or destruction is not feasible. The obligations of Contractor under this Agreement to protect PII and to limit its use or disclosure shall continue and shall survive until all PII is either returned to the Exchange or destroyed.