EXHIBIT M

BUSINESS ASSOCIATE AGREEMENT ("BAA")

Contractor is a business associate ("BA") as defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH") and shall comply with the additional terms and conditions set forth in this Exhibit M to the _____ ("Agreement"). This Business Associate Agreement Exhibit "M" supplements and is made a part of the Contract by and between the County of Marin, referred to herein as Covered Entity ("CE") and _____, referred to herein as Business Associate ("BA"), to which this Exhibit "M" is an incorporated attachment.

RECITALS

WHEREAS, the County of Marin is either a "covered entity" or "business associate" of a covered entity as each are defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended by the HITECH Act, as defined below, and the related regulations promulgated by the United States Department of Health and Human Services (collectively, "HIPAA") and, as such, is required to comply with the HIPAA's provisions regarding confidentiality and privacy of Protected Health Information as defined herein.

WHEREAS the Business Associate and Covered Entity acknowledge that the fulfillment of the Parties' obligations under this Agreement necessitates the exchange of, or access to, data including Protected Health Information (PHI), as defined herein.

WHEREAS, the Parties have entered or will enter into one or more agreements under which Business Associate provides or will provide certain specified services to Covered Entity (collectively, the "Agreement").

WHEREAS, in providing services pursuant to the Agreement, Business Associate will have access to Protected Health Information.

WHEREAS, by providing the services pursuant to the Agreement, Business Associate will become a "business associate" of the Covered Entity as such term is defined under HIPAA.

WHEREAS, both Parties are committed to complying with all federal and state laws governing the confidentiality and privacy of health information, including, but not limited to, the Standards for Privacy of Individually Identifiable Health Information found at 45 CFR Part 160 and Part 164, Subparts A and E (collectively, the "Privacy Rule"); including PHI related to lawful reproductive health care. This includes information about contraception, fertility treatments, and pregnancy related care, and

WHEREAS, both Parties intend to protect the privacy and provide for the security of Protected Health Information disclosed to Business Associate pursuant to the terms of this Agreement, HIPAA, and other applicable laws.

AGREEMENT

NOW, THEREFORE, in consideration of the mutual covenants and conditions contained herein and the continued provision of PHI by Covered Entity to Business Associate under the Agreement in reliance on this BAA, the Parties agree as follows:

I. **Definitions:**

a. **Catch-all definition:** The following terms and others used in this Agreement shall have the same meaning as in the HIPAA Privacy and Security Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, HHS Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

b. **"Access"** means the ability or the means necessary to read write, modify, or communicate data/information or otherwise use any system resource.

c. **"Affiliate"** means a subsidiary or affiliate of Covered Entity that is, or has been, considered a covered entity, as defined by HIPAA.

d. **"Breach"** means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI, as defined in 45 CFR §164.402.

e. **"Breach Notification Rule"** means the portion of HIPAA set forth in Subpart D of 45 CFR Part 164.

f. **Business Associate** a covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information.

g. **Confidential Information** shall mean all non-public, medical, financial, and personal information in whatever form (written, oral, visual, or electronic) possessed or obtained by either party. Confidential Information shall include all information which,

   i. either party has labeled in writing as confidential,
   ii. is identified at the time of disclosure as confidential,
   iii. is commonly regarded as confidential in the health care industry, or
   iv. is PHI as defined by HIPAA.

h. **Covered Entity** shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. Section 160.103. and 42CFR Part 2. For purposes of this Contract, this term is intended to mean the County of Marin.

i. **"Data Aggregation"** "shall be consistent with the meaning given to that term in the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

j. **"De-Identify"** means to alter the PHI such that the resulting information meets the requirements described in 45 CFR §§164.514(a) and (b).

k. **"Designated Record Set"** has the meaning given to such term under the Privacy Rule, including 45 CFR §164.501. B.

l. **DHHS Secretary** shall mean the Secretary of the U.S. Department of Health and Human Services.

m. **"Electronic PHI" or "e-PHI"** means any PHI maintained in or transmitted by electronic media as defined in 45 CFR §160.103.
n. **"Health Care Operations**" has the meaning given to such term under the Privacy Rule, defined in 45 CFR §164.501.
o. **"HHS"** means the U.S. Department of Health and Human Services.
p. **HIPAA Rules** shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
q. **"HITECH Act"** means the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, Public Law 111-005.
r. **"Individual"** has the same meaning given to that term I in 45 CFR §§164.501 and 160.130 and includes a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).
s. **"Privacy Rule"** means that portion of HIPAA set forth in 45 CFR Part 160 and Part 164, Subparts A and E.
t. **"Protected Health Information" or "PHI"** has the meaning given to the term "protected health information" in 45 CFR §§164.501 and 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
u. **"Reproductive Health Records"** HIPAA Privacy Rule supports reproductive health care privacy. The business associate must comply with the requirements applicable to the covered entity's obligation under the HIPAA Privacy Rule.
v. **"Security Incident"** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
w. **"Security Rule"** means the Security Standards for the Protection of Electronic Health Information provided in 45 CFR Part 160 & Part 164, Subparts A and C.
x. **Technical Safeguards** means the technology and the policy and procedures for its use that protect e-PHI and control access to it.
y. **"Unsecured Protected Health Information" or "Unsecured PHI"** means any "protected health information" as defined in 45 CFR §§164.501 and 160.103 that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals using a technology or methodology specified by the HHS Secretary in the guidance issued pursuant to the HITECH Act and codified at 42 USC §17932(h).

II. **Permitted Use and Disclosures of PHI**.
a. **Permitted Uses.** BA shall not use Protected Information except for the purpose of performing BA's obligations under the Contract and as permitted under the Contract and this Exhibit "M". Further, and notwithstanding anything to the contrary above, BA shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so used by CE. However, BA may use Protected Information (i) for the proper management and administration of BA, (ii) to carry out the legal responsibilities of BA, or (iii) for Data Aggregation purposes for the Health Care Operations of CE [45 C.F.R. Sections 164.504(e)(2)(ii)(A) and 164.504(e)(4)(i)].
b. **Permitted Disclosures.** BA shall not disclose PHI except for the purpose of performing the Business Associate's obligations under the Contract and as permitted under the Contract and this Exhibit "M". Furthermore, the Business Associate shall not disclose PHI in any manner that would constitute a violation

of the Privacy Rule or the HITECH Act if so, disclosed by the Covered Entity. However, the Business may disclose PHI in the following circumstances:

- For the proper management and administration of the Business Associate
- To carry out the legal responsibilities of the Business Associate.
- As required by law,
- For Data Aggregation purposes for the Health Care Operations of the Covered Entity.

  If the Business Associate discloses PHI to a third party, the Business Associate must obtain, prior to making any such disclosure:

  (i) Reasonable written assurances from the third party that PHI will be held confidential as provided pursuant to this Exhibit "M" and only disclosed as required by law or for the purposes for which it was disclosed to such third party.

  (ii) A written agreement from the third party to immediately notify the Business Associate of any breaches of confidentiality of the PHI, to the extent the third party has knowledge of such breach [42 U.S.C. Section 17932; 45 C.F.R. Sections 164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)].

III. **Prohibited Uses and Disclosures of PHI.**

a. The Business Associate shall not use or disclose PHI for fundraising or marketing purposes. The Business Associate shall not disclose PHI to a health plan for payment or health care operations purposes if the patient has requested a special restriction and has paid out of pocket in full for the health care item or service to which the PHI solely relates, as per 42 U.S.C. Section 17935(a). BA shall not directly or indirectly receive remuneration in exchange for Protected Information, except with the prior written consent of CE and as permitted by the HITECH Act, 42 U.S.C. section 17935(d)(2); however, this prohibition shall not affect payment by CE to BA for services provided pursuant to the Contract.

b. Business Associate will not use or disclose PHI in a manner other than as provided in this BAA, as permitted under the Privacy Rule, or as required by law. Business Associate will use or disclose PHI, to the extent practicable, as a limited data set or limited to the minimum necessary amount of PHI to carry out the intended purpose of the use or disclosure, in accordance with Section 13405(b) of the HITECH Act (codified at 42 USC §17935(b)) and any of the act's implementing regulations adopted by HHS, for each use or disclosure of PHI.

III. **Sell or Exchange PHI for Remuneration**. BA shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of HHS and as permitted by 42 U.S.C. section 17935(d) (2).

IV. **Safeguards Against Misuse of PHI**. Business Associate will use appropriate safeguards to prevent the use or disclosure of PHI other than as provided by the Agreement or this BAA and Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity. Business Associate agrees to take reasonable steps, including providing adequate training to its employees to ensure compliance with this BAA and to ensure that

the actions or omissions of its employees or agents do not cause Business Associate to breach the terms of this BAA.

V. Reporting Disclosures of PHI and Security Incidents. Business Associate will report to Covered Entity in writing any use or disclosure of PHI not provided for by this BAA of which it becomes aware. This report shall be made to the HHS Contract Manager, the Compliance Privacy Officer, and the HHS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday, notice shall be provided by calling the HHS-IST Service Desk immediately. Business Associate agrees to report any such event no later than five (5) business days of becoming aware of the event.

- HHS Compliance & Privacy Officer: HHSCompliance@MarinCounty.Gov
- HHS Information Security Officer: HHS-CISO@MarinCounty.Gov

VI. Reporting Breaches of Unsecured PHI.

1. **Notification of Improper Access, Use or Disclosure and Breach**. Unless stricter reporting requirements apply under federal or state laws or regulations, other provisions of the Contract, or this Exhibit "M", the Business Associate must report to the Covered Entity any unauthorized access, use or disclosure of PHI suspected and actual breaches of PHI, and security incidents involving PHI.
2. **Initial Notice.** An Initial Notice must be provided to the Covered Entity within five (5) business days of any suspected or actual breach of security, intrusion or unauthorized use or disclosure of PHI. This includes any suspected or actual access, use or disclosure of data in violation of the Contract and this Exhibit "M" and/or any applicable federal or state laws or regulations. The Initial Notice must include:

- Date of incident
- Date of discovery
- PHI/data elements involved
- mode of disclosure (e.g. verbal, paper, electronic)
- Circumstance of release
- Recipient
- Mitigation efforts
- Corrective action take

The Business Associate shall:

- Immediately investigate breaches and security incidents involving protected information,
- Take prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the operating environment.
- Comply with all relevant federal and state laws and regulations regarding unauthorized disclosure.

The parties agree that the Covered Entity has the sole discretion to determine whether it will undertake such obligations on behalf of the Business Associate and that, if it does, the Covered Entity has the right to require the Business Associate to pay for any reasonable costs associated therewith. The Business Associate shall provide notice to the Covered Entity as set forth in paragraph 6.

3. **Complete Report** A complete report must be submitted within ten (10) working days of the discovery. This report shall include any required not available at the time the Initial Notice and summary of the investigation. The summary should include an assessment of all known factors relevant to determining whether a breach occurred under applicable HIPAA provisions and/or other applicable law. To the extent feasible, based on the investigation, the report shall also include a Corrective Action Plan (CAP) with detailed information regarding the mitigation measures taken to halt and/or contain the improper use or disclosure. The Business Associate shall provide any other reasonable and relevant requested information.
4. **Notification of Individuals and Regulatory Agencies**. When the breach is caused by the Business Associate or its subcontractor and applicable state or federal law requires notification to individuals and reporting of a breach or unauthorized disclosure of PHI, the Business Associate shall provide the required notice and report pursuant to the applicable state or federal requirements. Notifications must be made without unreasonable delay and in any event, no later than sixty (60) calendar days from notifying the Covered Entity of the Breach.

VII. **Mitigation of Disclosures of PHI**. Business Associate will take reasonable measures to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of any use or disclosure of PHI by Business Associate or its agents or subcontractors in violation of the requirements of this BAA. Sanctions and/or Penalties. The Business Associate understands that a failure to comply with the provisions of HIPAA, the HITECH Act, and the HIPAA regulations that are applicable to BA may result in the imposition of sanctions and/or penalties on the Business associate under HIPAA the HITECH Act.

VIII. **Agreements with Agents or Subcontractors**. The Business Associate will ensure that any agents or subcontractors with access to, or provided with, PHI agree in writing to the restrictions and conditions on the use and disclosure of PHI outlined in this BAA. They will also implement reasonable and appropriate safeguards to protect any Electronic PHI created, received, maintained, or transmitted on behalf of Business Associate or, through the Business Associate. The Business Associate shall notify the Covered Entity, or upstream Business Associate, of all subcontracts and agreements involving PHI within 30 (thirty) calendar days of execution. This notification will be posted on the Business Associate's primary website. The Business Associate will ensure that all subcontracts and agreements provide the same level of privacy and security as this BAA.

IX. **Audits, Inspection and Enforcement.** Within ten (10) days of a written request by the Covered Entity, the Business Associate and its agents or subcontractors shall allow the Covered Entity to conduct a reasonable inspection of their facilities, systems, books, records, agreements, contracts, policies, and procedures relating to the use or disclosure of Protected Health Information specified in this Exhibit "M." This inspection aims to determine whether BA has complied with this Exhibit. The following conditions apply:

- The Business Associate and the Covered Entity must mutually agree in advance on the scope, timing, and location of such an inspection,
- The Covered Entity must protect the confidentiality of all the Business Associate's confidential and proprietary information during inspection.
- The Covered Entity must execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by the Business Associate.

The fact that the Covered Entity inspects, or fails to inspect, the Business associate's facilities, systems, books, records, agreements, contracts, policies, and procedures does not relieve the Business Associate of its responsibility to comply with this Exhibit "M." the Covered Entity's failure to detect or notify the Business Associate of unsatisfactory practices does not constitute acceptance of such practice or a waiver of the Covered Entity's enforcement rights under the Contract or this Exhibit "M".

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

X. Access to PHI by Individuals. Upon request, the Business Associate agrees to provide Covered Entity with copies of the PHI maintained by Business Associate in a Designated Record Set. This must be done in the time and manner specified by the Covered Entity, enabling the Covered Entity to respond to an Individual's request for access to PHI under 45 CFR §164.524.
If an Individual or their personal representative requests access to the Individual's PHI directly from the Business Associate, the Business Associate will forward that request to the Covered Entity within ten business days.
Any decision to disclose or not disclose the PHI requested by an Individual or their personal representative and complies with the requirements related to an Individual's right to access PHI, is the sole responsibility of Covered Entity.

XI. Amendment of PHI. Upon request and instruction from the Covered Entity, the Business Associate will amend PHI or a record about an Individual in a Designated Record Set that is maintained by, or otherwise within the possession of, the Business Associate as directed by Covered Entity in accordance with procedures established by 45 CFR §164.526. Any request by Covered Entity to amend such information will be completed by the Business Associate within 15 business days of Covered Entity's request.

If an Individual requests that Business Associate amend their PHI or record in a Designated Record Set, the Business Associate will forward this request to Covered Entity within ten business days. Any amendment of, or decision not to amend, the PHI or record as requested by an Individual and complies with the requirements applicable to an Individual's right to request an amendment of PHI will be the sole responsibility of Covered Entity.

XII. Accounting of Disclosures. The Business Associate will document any disclosures of PHI it makes, as required by 45 CFR §164.528(a). It will also provide information related to these disclosures to the Covered Entity to enable them to respond to a request for an accounting of disclosures in accordance with 45 CFR §164.528. At a minimum, the Business Associate will provide the Covered Entity with the following for any covered disclosures:

- The date of disclosure of PHI.
- The name of the entity or person who received PHI, and, if known, their address.
- A brief description of the PHI disclosed.
- A brief statement of the purpose of the disclosure, including the basis for such disclosure.

The Business Associate will furnish the Covered Entity with this information within ten business days after receiving a written request from the Covered Entity. This is to allow the Covered Entity to make an accounting of disclosures as required by 45 CFR §164.528.

If the Covered Entity elects to provide an Individual with a list of its business associates, the Business Associate will provide an accounting of its disclosures of PHI upon the Individual's request. if and to the extent required under the HITECH Act or related HHS regulations.
If an Individual submits an initial request for an accounting directly to the Business Associate, the Business Associate will forward this request to Covered Entity within ten business days.

XIII. **Availability of Books and Records**. The Business Associate will make available its internal practices, books, agreements, records, and policies and procedures relating to the use and disclosure of PHI, to the Secretary of HHS upon request. This is to allow the determination of both the Covered Entity's and Business Associate's compliance with HIPAA, and this BAA.

XIV. **Responsibilities of Covered Entity**. Regarding the use and/or disclosure of PHI by the Business Associate, Covered Entity agrees to:

1. **Notify** the Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
2. **Notify** the Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
3. **Notify** the Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.
4. **Refrain from requesting** the Business Associate to use or disclose PHI in a manner that would not be permissible under HIPAA if done by Covered Entity, except for data aggregation or management and administrative activities by the Business Associate.

XV. **Data Ownership**. Business Associate's data stewardship does not confer data ownership rights on Business Associate with respect to any data shared with it under the Agreement, including all forms thereof.

XVI. **Term and Termination.** This BAA will become effective on the date the Agreement is executed and will remain in effect until all obligations of the Parties have been met under both the Agreement and under this BAA.

1. **Material Breach**. A breach by the Business associate of any provision of this Exhibit "M", as determined by the Covered Entity, shall constitute a material breach of the Contract, and shall provide grounds for immediate termination of the Contract, notwithstanding any contrary provision in the Contract or this Agreement. [45 C.F.R. Section 164.504(e)(2)(iii)].
2. **Judicial or Administrative Proceedings**. The Covered Entity CE may terminate the Contract, effective immediately, if (i) BA is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, HIPAA Regulations or other security or privacy laws or (ii) there is a finding or stipulation that the BA has violated any standard or requirement of HIPAA, the HITECH Act, the HIPAA Regulations or other security or privacy laws in any administrative or civil proceeding in which the Business associate has been joined.

3. **Effect of Termination**. Upon termination of the Contract for any reason, the Business Associate shall, at the option of the Covered Entity, return or destroy all PHI that the Business Associate or its agents or subcontractors still maintain in any form, and shall retain no copies of such PHI. If return or destruction is not feasible, as determined by the Covered Entity, the Business Associate, shall continue to extend the protections of Section 2 of this Exhibit "M" to such information, and limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. If the Covered Entity elects destruction of the PHI, the Business Associate shall certify in writing to the Covered Entity that such PHI has been destroyed. [45 C.F.R. Section 164.504(e)(ii)(2(I)].

XVII. **Effect of BAA.** This BAA is a part of and subject to the terms of the Agreement. In case of any conflict with any terms of this BAA and Agreement, the terms of this BAA will govern. Except as expressly stated in this BAA or as provided by law, this BAA does not create any rights in favor of any third party.

XVIII. **Regulatory References**. A reference in this BAA to a section in the HIPAA regulations means the section as currently in effect or as amended.

XIX. **Indemnification.** In addition to any other indemnification and defense obligation under the Contract, the Business Associate will indemnify, defend and hold harmless the Covered Entity and its employees, directors, officers, subcontractors, agents and affiliates from and against all claims, actions, damages, losses, liabilities, fines, penalties, costs or expenses, including reasonable attorney's fees, incurred by the Covered Entity from or in connection with any breach of Exhibit "M", or any negligent or wrongful acts or omissions by the Business Associate or its employees, directors, officers, subcontractors or agents.

XX. **Notices**. All notices, requests, demands, or other communications under this BAA must be made via either first-class mail, registered or certified mail or express courier, or electronic mail.

XXI. **Amendments and Waiver**. This BAA may not be modified, nor will any provision be waived or amended, except in writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

XXII. **HITECH Act Compliance**. The Parties acknowledge that the HITECH Act includes significant changes to the Privacy Rule and the Security Rule. The HITECH Act sets forth provisions that significantly change the requirements for business associates and the agreements between business associates and covered entities under HIPAA and these changes may be further clarified in forthcoming regulations and guidance. Each Party agrees to comply with the applicable provisions of the HITECH Act and any HHS regulations issued with respect to the HITECH Act. The Parties also agree to negotiate in good faith to modify this BAA as reasonably necessary to comply with the HITECH Act and its regulations as they become effective. If the Parties are unable to reach agreement on such a modification, either Party will have the right to terminate this BAA upon 30-days' prior written notice to the other Party.

EFFECTIVE DATE AND EXECUTION

This BAA shall be agreed to and effective upon execution of the Agreement number to which it is attached as an Exhibit M and is incorporated by reference thereto.

Business Associate Representative:

Name: _____

Title: _____

Signature: _____

County of Marin Contract Manager or Designee:

Name: _____

Title: _____

Signature: _____