

**EXHIBIT M:
BUSINESS ASSOCIATE AGREEMENT
TERMS AND CONDITIONS**

To the extent Contractor is a business associate as defined under the Federal Health Insurance Portability and Accountability Act (“HIPAA”) and the HITECH Act, Contractor shall comply with the additional terms and conditions set forth in this Exhibit (“M”) to the Professional Services Contract (“PSC” or “Contract”). 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

CE and BA have entered into a business relationship through which BA may receive Protected Health Information (“PHI”) (defined below) from CE or create, collect, transmit, retain, process or otherwise use PHI on behalf of CE pursuant to the terms of the Contract.

CE and BA intend to protect the privacy and provide for the security of PHI disclosed to, created by, or in any manner used by, BA pursuant to the Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (“the HITECH Act”), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the “HIPAA Regulations”) and other applicable laws.

As part of the HIPAA Regulations, the Privacy Rule and the Security Rule (defined below) require CE to enter into a contract containing specific requirements with BA prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(e) and 164.504(e) of the Code of Federal Regulations (“C.F.R.”) and contained in this Exhibit “M”.

In consideration of the mutual promises below and the exchange of information pursuant to this Exhibit “M”, the parties agree as follows:

1. Definitions

- a. **Breach** shall have the meaning given to such term under the HITECH Act [42 U.S.C. Section 17921].
- b. **Business Associate** shall have the meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including but not limited to, 42 U.S.C. Section 17938 and 45 C.F.R. Section 160.103. For purposes of this Exhibit “M”, use of the term Business Associate includes all Contractor agents, employees, contractors or other associates providing services or assistance to Contractor under the Contract.
- c. **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. For purposes of this Contract, this term is intended to mean the County of Marin.
- d. **Data Aggregation** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

- e. **Designated Record Set** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.
- f. **DHHS Secretary** shall mean the Secretary of the U.S. Department of Health and Human Services.
- g. **Electronic Health Record** shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921.
- h. **Electronic Protected Health Information** means Protected Health Information that is maintained in or transmitted by electronic media.
- i. **Health Care Operations** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.
- j. **Individual** 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.
- k. **Privacy Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.
- l. **Protected Health Information or PHI** means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental 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; and (ii) that identifies the Individual or with respect to which there is a reasonable basis to believe the information can be used to identify the Individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501. Protected Health Information includes Electronic Protected Health Information [45 C.F.R. Sections 160.103, 164.501].
- m. **Protected Information** shall mean PHI provided by CE to BA or created or received by BA on CE's behalf.
- n. **Security Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.
- o. **Unsecured PHI** shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h).

2. Obligations of Business Associate

- 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 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 disclose Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so disclosed by CE. However, BA may disclose Protected Information (i) for the proper management and administration of BA; (ii) to carry out the legal responsibilities of BA; (iii) as required by law; or (iv) for Data Aggregation purposes for the Health Care Operations of CE. If BA discloses Protected Information to a third party, BA must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such Protected Information 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, and (ii) a written agreement from such third party to immediately notify BA of any breaches of confidentiality of the Protected Information, to the extent it has obtained 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)].
- c. Prohibited Uses and Disclosures.** BA shall not use or disclose Protected Information for fundraising or marketing purposes. BA shall not disclose Protected Information to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates 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.
- d. Appropriate Safeguards.** BA shall implement appropriate administrative, physical and technical safeguards as are necessary to prevent the use or disclosure of Protected Information otherwise than as permitted by the Contract that reasonably and appropriately protect the confidentiality, integrity and availability of the Protected Information, in accordance with 45 C.F.R. Sections 164.308, 164.310, and 164.312. [45 C.F.R. Section 164.504(e)(2)(ii)(B); 45 C.F.R. Section 164.308(b)]. BA shall comply with the policies and procedures and documentation requirements of the Security Rule, including, but not limited to, 45 C.F.R. Section 164.316. [42 U.S.C. Section 17931]
- e. Reporting of Improper Access, Use or Disclosure.** Unless stricter reporting requirements apply in accordance with federal or state laws or regulations, other provisions of the Contract, or this Exhibit "M", BA shall report to CE in writing of any access, use or disclosure of Protected Information not permitted by the Contract and this Exhibit "M", and any Breach of Unsecured PHI of which it becomes aware without unreasonable delay and in no case later than five **(5) business days** after discovery [42 U.S.C. Section 17921; 45 C.F.R. Section 164.504(e)(2)(ii)(C); 45 C.F.R. Section 164.308(b)]. BA shall provide notice to CE as set forth in paragraph 6.
- f. Business Associate's Agents.** BA shall ensure that any agents, including subcontractors, to whom it provides Protected Information, agree in writing to the same restrictions and conditions that apply to BA with respect to such PHI and implement the safeguards required by paragraph d above with respect to PHI [45 C.F.R. Section 164.504(e)(2)(ii)(D); 45 C.F.R. Section 164.308(b)]. BA shall implement and maintain

sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation (see 45 C.F.R. Sections 164.530(f) and 164.530(e)(1)).

- g. Access to Protected Information.** BA shall make Protected Information maintained by BA or its agents or subcontractors in Designated Record Sets available to CE for inspection and copying within ten (10) business days of a request by CE to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.524 [45 C.F.R. Section 164.504(e)(2)(ii)(E)]. If BA maintains an Electronic Health Record, BA shall provide such information in electronic format to enable CE to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. Section 17935(e). If any Individual requests access to protected Information directly from BA or its agents or subcontractors, BA shall inform the CE of the request without unreasonable delay, in any event no later than three (3) days of receipt of the request. If the CE permits the disclosure, the CE will inform the BA within two (2) days of the receipt of the request from BA, Whereupon the BA will be authorized to provide access to the client.
- h. Amendment of PHI.** Within ten (10) business days of receipt of a request from CE for an amendment of Protected Information or a record about an Individual contained in a Designated Record Set, BA or its agents or subcontractors shall make such Protected Information available to CE for amendment and incorporate any such amendment to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.526. If any Individual requests an amendment of Protected Information directly from BA or its agents or subcontractors, BA must notify CE in writing within five (5) business days of the request. Any approval or denial of amendment of Protected Information maintained by BA or its agents or subcontractors shall be the responsibility of CE [45 C.F.R. Section 164.504(e)(2)(ii)(F)].
- i. Accounting Rights.** Within ten (10) business days of notice by CE of a request for an accounting of disclosures of Protected Information, BA and its agents or subcontractors shall make available to CE the information required to provide an accounting of disclosures to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.528, and the HITECH Act, including but not limited to 42 U.S.C. Section 17935(c), as determined by CE. BA agrees to implement a process that allows for an accounting to be collected and maintained by BA and its agents or subcontractors for at least six (6) years prior to the request. However, accounting of disclosures from an Electronic Health Record for treatment, payment or health care operations purposes are required to be collected and maintained for only three (3) years prior to the request, and only to the extent that BA maintains an Electronic Health Record and is subject to this requirement. At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed and (iv) a brief statement of purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the Individuals' authorization, or a copy of the written request for disclosure. In the event that the request for an accounting is delivered directly to BA or its agents or subcontractors, BA shall within five (5) business days of a request forward it to CE in writing. However, it shall be BA's responsibility to prepare and deliver any such accounting requested and to do so in accordance with law. BA shall not disclose any Protected Information except as set forth in Sections 2.b. of this Exhibit "M" [45 C.F.R. Sections 164.504(e)(2)(ii)(G) and 165.528].

- j. Governmental Access to Records.** BA shall make its internal practices, books and records relating to the use, disclosure and privacy protection of Protected Information available to CE and to the DHHS Secretary for purposes of determining BA's compliance with the Privacy Rule [45 C.F.R. Section 164.504(e)(2)(ii)(H)]. BA shall provide to CE a copy of any Protected Information that BA provides to the DHHS Secretary concurrently with providing such Protected Information to the DHHS Secretary.
- k. Minimum Necessary.** BA and its agents or subcontractors shall request, use and disclose only the minimum amount of Protected Information necessary to accomplish the purpose of the request, use, or disclosure. [42 U.S.C. Section 17935(b); 45 C.F.R. Section 164.514(d)(3)] BA understands and agrees that the definition of "minimum necessary" is in flux and shall keep itself informed of guidance issued by the DHHS Secretary with respect to what constitutes "minimum necessary."
- l. Data Ownership.** BA acknowledges that BA has no ownership rights with respect to the Protected Information. The CE is the owner of all protected information and/or records containing such PHI provided to BA pursuant to the Contract or this Exhibit "M."
- m. Notification of Breach.** Unless stricter reporting requirements apply in accordance with federal or state laws or regulations, other provisions of the Contract, or this Exhibit "M", BA shall notify CE within twenty-four (24) hours of any suspected or actual breach of security, intrusion or unauthorized use or disclosure of PHI of which BA becomes aware and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. Unless CE provides BA with written notice within **3 (three) business days** that it will undertake such obligations on behalf of BA, BA shall take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations. The parties agree that CE has the sole discretion to determine whether or not it will undertake such obligations on behalf of BA and that, if it does, CE has the right to require BA to pay for any or all costs associated therewith. BA shall provide notice to CE as set forth in paragraph 6.
- n. Breach Pattern or Practice by Covered Entity.** Pursuant to 42 U.S.C. Section 17934(b), if the BA knows of a pattern of activity or practice of the CE that constitutes a material breach or violation of the CE's obligations under the Contract or this Exhibit "M" or other arrangement, the BA must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, the BA must terminate the Contract or other arrangement if feasible, or if termination is not feasible, report the problem to the DHHS Secretary. BA shall provide written notice to CE of any pattern of activity or practice of the CE that BA believes constitutes a material breach or violation of the CE's obligations under the Contract or this Exhibit "M" or other arrangement within five (5) business days of discovery and shall meet with CE to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation. BA shall provide notice to CE as set forth in paragraph 6.
- o. Audits, Inspection and Enforcement.** Within ten (10) days of a written request by CE, BA and its agents or subcontractors shall allow CE to conduct a reasonable inspection of the facilities, systems, books, records, agreements, contracts, policies and procedures relating to the use or disclosure of Protected Information pursuant to this Exhibit "M" for the purpose of determining whether BA has complied with this Exhibit; provided,

however, that (i) BA and CE shall mutually agree in advance upon the scope, timing and location of such an inspection, (ii) CE shall protect the confidentiality of all confidential and proprietary information of BA to which CE has access during the course of such inspection; and (iii) CE shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by BA. The fact that CE inspects, or fails to inspect, or has the right to inspect, BA's facilities, systems, books, records, agreements, contracts, policies and procedures does not relieve BA of its responsibility to comply with this Exhibit "M", nor does CE's (i) failure to detect or (ii) detection, but failure to notify BA or require BA's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of CE's enforcement rights under the Contract or this Exhibit "M". BA shall notify CE within ten (10) business days of learning that BA has become the subject of an audit, compliance review, or complaint investigation by the Office for Civil Rights.

3. Termination of Contract

- a. **Material Breach.** A breach by BA of any provision of this Exhibit "M", as determined by CE, shall constitute a material breach of the Contract and shall provide grounds for immediate termination of the Contract, any provision in the Contract to the contrary notwithstanding. [45 C.F.R. Section 164.504(e)(2)(iii)].
- b. **Judicial or Administrative Proceedings.** Notwithstanding any provision in the Contract to the contrary, 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, the HIPAA Regulations or other security or privacy laws or (ii) 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 is made in any administrative or civil proceeding in which the party has been joined.
- c. **Effect of Termination.** Upon termination of the Contract for any reason, BA shall, at the option of CE, return or destroy all Protected Information that BA or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If return or destruction is not feasible, as determined by CE, BA 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. [45 C.F.R. Section 164.504(e)(ii)(2)(I)]. If CE elects destruction of the PHI, BA shall certify in writing to CE that such PHI has been destroyed.

4. Indemnification

In addition to any other indemnification and defense obligation under the Contract, BA will indemnify, defend and hold harmless CE and its respective employees, directors, officers, subcontractors, agents and affiliates from and against all claims, actions, damages, losses, liabilities, fines, penalties, costs or expenses, including without limitation reasonable attorney's fees, suffered by CE from or in connection with any breach of Exhibit "M", or any negligent or wrongful acts or omissions in connection with this Exhibit "M", by BA or its employees, directors, officers, subcontractors or agents.

5. Insurance

BA shall maintain insurance with respect to BA's obligations under the Contract and this Exhibit "M" reasonably satisfying to CE and provide from time to time as requested by CE proof of such insurance.

6. Notices

Any notice to be given under this Exhibit "M" to CE shall be made via overnight mail or hand delivery at CE's address given below and by providing telephonic notification as specified below. Any such notice shall be deemed given when so delivered to or received at the proper address.

Notice to CE:

- a. Privacy Officer – Department of Health and Human Services, 20 N. San Pedro Rd, San Rafael, CA 94903.
- b. Compliance and breach reporting line – (415) 473-6948.

Notice to BA:

[insert address]

7. Disclaimer

CE makes no warranty or representation that compliance by BA with this Exhibit "M", HIPAA, the HITECH Act, or the HIPAA Regulations will be adequate or satisfactory for BA's own purposes. BA is solely responsible for all decisions made by BA regarding the safeguarding of PHI.

8. Certification

To the extent that CE determines that such examination is necessary to comply with CE's legal obligations pursuant to HIPAA relating to certification of its security practices, CE or its authorized agents or contractors, may, at CE's expense, examine BA's facilities, systems, procedures and records as may be necessary for such agents or contractors to certify to CE the extent to which BA's security safeguards comply with HIPAA, the HITECH Act, the HIPAA Regulations or this Exhibit.

9. Amendment

- a. **Amendment to Comply with Law.** The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of the Contract or this Exhibit "M" 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, the Privacy Rule, the Security Rule and other applicable laws relating to the security or confidentiality of PHI. The parties understand and agree that CE must receive satisfactory written assurance from BA that BA will adequately safeguard all Protected Information. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Exhibit "M" embodying written assurances consistent with the standards and requirements of HIPAA, the

HITECH Act, the Privacy Rule, the Security Rule or other applicable laws. CE may terminate the Contract upon thirty (30) days written notice in the event (i) BA does not promptly enter into negotiations to amend the Contract or this Exhibit "M" when requested by CE pursuant to this Section or (ii) BA does not enter into an amendment to the Contract or this Exhibit "M" providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of applicable laws.

- b. Amendment of Exhibit "M".** This Exhibit "M" may be modified or amended at any time without amendment of the Contract, but only by written agreement of the parties.

10. Assistance in Litigation of Administrative Proceedings

BA shall make itself, and any subcontractors, employees or agents assisting BA in the performance of its obligations under the Contract, available to CE, at no cost to CE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, 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 BA or its subcontractor, employee or agent is a named adverse party.

11. No Third-Party Beneficiaries

Nothing expressed or implied in the Contract or this Exhibit "M" is intended to confer, nor shall anything herein confer, upon any person other than CE, BA and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

12. Effect on Contract

Except as specifically required to implement the purposes of this Exhibit "M", or to the extent inconsistent with this Exhibit "M", all other terms of the Contract shall remain in force and effect.

13. Interpretation

The provisions of this Exhibit "M" shall prevail over any provisions in the Contract that may conflict or appear inconsistent with any provision in this Exhibit "M". This Exhibit "M" and the Contract shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the Privacy Rule and the Security Rule. The parties agree that any ambiguity in this Exhibit "M" shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act, the Privacy Rule and the Security Rule.

14. Survival of Provisions

Excepting only the provisions regarding BA's use or disclosure of Protected Information for the purpose of performing BA's obligations under the Contract, the terms of this Exhibit "M" shall survive the termination of the Contract so long as PHI obtained or generated during the term of the Contract is retained by BA.