MEDICAL INSURANCE EXCHANGE OF CALIFORNIA
BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is made and effective between Medical Insurance Exchange of California and Medical Underwriters of California, Attorney-in-Fact for MIEC, (hereinafter "MIEC") ("Business Associated" or "BA") and persons or entities insured under an MIEC policy of insurance who, as a "Covered Entity" or "CE" who provide Protected Health Information ("PHI") to MIEC. This Agreement is intended to be a written arrangement between MIEC and CE to provide assurance to CE that MIEC shall properly safeguard any PHI provided by CE to MIEC consistent with 45 CFR §164.502(e)(2). By posting this Agreement on its website MIEC agrees to be bound by and comply with the terms of this Agreement to same extent as if this Agreement were signed by both parties and CE may reasonably rely on MIEC's commitment.

The purpose of this Agreement is to comply with all of the requirements and Standards for Privacy of Individually Identifiable Health Information (the "Privacy Regulations") and Security Regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH") Standards, as well as applicable laws of the state in which the CE is insured by BA as they may be amended from time to time, to ensure the integrity and confidentiality of individually identifiable personal and health information that BA may create for, or receive from, CE. BA will comply with the administrative, physical and technical safeguards, as well as the Security Rule's Business Associate Agreement requirements in the same manner as those requirements apply to CE.

Pursuant to and in furtherance of the agreement to provide professional liability insurance coverage and legal services and representation, and to enable performance of such legal services and representation as described above, BA needs to obtain from CE, and CE needs to disclose to BA, certain personal and health information, some of which may constitute PHI. BA may also have to use and disclose such information to other persons, including subcontractors and agents, for the purpose of performing its obligations under its agreement to provide legal services and representation. In that regard, BA will make reasonable efforts to limit the use and disclosure of PHI to the minimum necessary to accomplish the intended purpose of the agreement between BA and CE, and BA will enter into BA agreements with all subcontractors and/or agents who are retained by BA and who will be given access to PHI.

This Agreement establishes, among other things, the permitted and required uses and disclosures of PHI by the BA and does not authorize BA to use or further disclose the PHI other than as permitted by CE, by the Individual, by this Agreement, or by law. (45 CFR §164.504(e)(2)(i).)

Therefore, intending to be bound hereby, the parties agree as follows:

SECTION 1: DEFINITIONS

Unless otherwise provided, the following terms have the same meanings as set forth in the HIPAA Regulations and HITECH Standards.

1.1 "Agreement" means this Business Associate Agreement between Business Associate and Covered Entity.

1.2 "Breach" means the unauthorized acquisition, access, use or disclosure of PHI in a manner not permitted under Part 164, Subpart E of the HIPAA Regulations or the laws of the state in which the CE is insured by BA. A breach does not occur where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information and as otherwise excepted in Section 13400(1)(B) of the HITECH Act and 45 CFR §164.402(2).

1.3 "**Business Associate" (BA)** means a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. For purposes of this Agreement, "Business Associate" means MEDICAL INSURANCE EXCHANGE OF CALIFORNIA or MIEC.

1.4 "**Covered Entity" (CE)** means an insured of MIEC.

1.5 "**Designated Record Set"** means a group of records maintained by or for CE that is (1) the medical records and billing records about Individuals maintained by or for CE, or (2) used, in whole or in part, by or for CE to make decisions about Individuals. For purposes of this definition, the term "record" includes any item, collection, or grouping of information that contains PHI and is maintained, collected, used, or disseminated by or for the CE. See also, definition set out in 45 CFR §164.501.

1.6 "**Electronic Health Record" (EHR)** means an electronic record of health-related information regarding an Individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

1.7 "**Electronic Protected Health Information" (ePHI)** means Protected Health Information that is transmitted by or maintained in electronic media or in electronic format.

1.8 "**HIPAA Regulations"** means the collective privacy and security regulations found at 45 CFR Parts 160 and 164, promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 140-191.

1.9 "**HITECH Standards"** means the privacy and security provisions applicable to Business Associates under Subtitle D of the Health Information Technology for Economic and Clinical Health Act, set forth in Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 1115 ("HITECH Act"), and any regulations promulgated thereunder.

1.10 "**Individual"** means the person who is the subject of PHI and includes a person who qualifies as a personal representative in accordance with the HIPAA Regulations and HITECH Standards.

1.11 "**Protected Health Information" (PHI)** means either medical or individual information in electronic or physical form which (i) relates to the past, present, or future physical or mental health condition of an Individual, the provision of health care to an Individual, or the past, present, or future payment for the provision of health care to an Individual, (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual, and (iii) is limited to the information created or received by BA from or on behalf of CE (as defined by 45 CFR §164.501).

1.12 "**Secretary"** means the Secretary of the Department of Health and Human Services or his/her designee.

1.13 "**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. See definition in 45 CFR §164.304.

1.14 "Security Rule" means the security standards in 45 CFR Parts 160, 162 and 164, as amended, and related agency guidance.

1.15 "**Unsecured Protected Health Information"** means PHI that is not secured through the use of a technology or methodology specified in the Secretary's guidance or, if guidance is not available, PHI that is not secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized Individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

SECTION 2: OBLIGATIONS OF BUSINESS ASSOCIATE

2.1 Limit PHI Use. BA agrees not to use PHI provided by, or created or obtained on behalf of CE other than as permitted or required by this Agreement, or as required or allowed by law and agency guidance, or as otherwise permitted in writing by the CE.

2.2 Limit PHI Disclosure. BA agrees not to disclose PHI except as permitted or required by this Agreement or as required by law.

2.3 Comply with CE's privacy policies. BA shall comply with CE's confidentiality/privacy policies, including but not limited to any Notice of Confidentiality and Privacy Practices.

2.4 Use and Disclose Minimum Necessary. BA will take reasonable efforts to limit request, use, and disclosure of PHI to the minimum necessary to accomplish the intended purpose of the request, use, or disclosure, but only as required by the HIPAA Regulations and HITECH Act Section 13405(b). BA shall assess and determine what constitutes the minimum necessary to accomplish the intended purpose in accord with HIPAA, HIPAA Regulations and any applicable guidance issued by the Secretary.

2.5 Use Safeguards. BA agrees to establish and use reasonable safeguards to prevent use or disclosure of PHI other than as allowed by this Agreement or as otherwise required or allowed by law. BA agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that BA creates, receives, maintains, or transmits on behalf of the CE.

2.6 Report Inappropriate Uses or Disclosures of PHI. If BA becomes aware of any use or disclosure of PHI not permitted by this Agreement or by law, BA agrees to report such violation to CE.

2.7 Report Security Incidents and Breaches of Unsecured PHI. If BA becomes aware of a Security Incident or Breach of Unsecured PHI, BA agrees to notify CE in writing as soon as possible, but in no event more than three (3) days after BA becomes aware of any Breach of or Security Incident involving CE's PHI, except where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security. BA is deemed to have become aware of the Breach or Security Incident as of the first day on which such Breach or Security Incident is known or with the exercise of reasonable diligence would have been known to any person other than the person committing the Breach or Security Incident who is an employee, officer, or other agent of the BA. So that CE may notify the Individuals of the breach by BA, the notice from BA to CE must include the identification of the Individuals whose Unsecured PHI was the subject of the Breach or Security Incident; a brief description of what happened; the date of the Breach or Security Incident and the date of the discovery of the Breach or Security Incident, if known; a description of the types of Unsecured PHI that were involved in the Breach or Security Incident (such as full name, Social Security Number, date of birth, home address, account number, disability code, or types of information that were involved); any steps the Individuals should take to protect themselves from potential harm resulting from the Breach or Security Incident; a brief description of what CE and BA are doing to investigate the Breach or Security Incident, to mitigate losses, and to protect against further Breaches or Security Incidents; and contact procedures for Individuals to ask questions or learn additional information, which must include a toll-free telephone number, email address, website, or postal address. BA shall

cooperate in good faith with CE in the investigation of any Breach or Security Incident.

2.8 Promptly Take Corrective Actions and Mitigate Harmful Effects. In addition to the notification requirements in section 2.6 and 2.7 above, and with prior notice to CE, BA shall take prompt corrective action to remedy any Breach or Security Incident, mitigate, to the extent practicable, any harmful effect of a use or disclosure of PHI by BA in violation of this Agreement, and take any other action required by applicable federal and state laws and regulations pertaining to such Breach or Security Incident. BA will comply with all HIPAA breach notification requirements.

2.9 Require Compliance of Subcontractors and Agents. BA agrees that anytime PHI is provided or made available to any subcontractors or agents, BA shall provide only the minimum necessary PHI for the purpose of the covered transaction. BA further agrees to ensure that any agent or subcontractor to whom it provides PHI must first agree in writing to the same restrictions and conditions that apply through this Agreement with respect to such information.

2.10 Access to Information. To the extent BA maintains the Designated Record Set, BA agrees to provide access to PHI in the original Designated Record Set, during normal business hours, provided CE or the Individual delivers prior written notice to BA, at least twenty (20) calendar days in advance of requesting such access, but only to the extent required by 45 CFR §164.524. If BA maintains an EHR, BA shall provide such information in electronic format to enable CE to fulfill its obligations under Section 13405(e) of the HITECH Act. BA may charge a reasonable fee for the cost of producing, copying, and mailing.

2.11 Incorporate Amendments. Upon written request by CE, to the extent BA maintains the Designated Record Set, BA agrees to incorporate any amendment(s) to PHI in the original Designated Record Set that CE requests or approves within twenty (20) calendar days after receipt of a written request pursuant to 45 CFR §164.526. Except as provided herein, BA shall not modify any existing data to which it is granted access other than to correct errors, or derive new data from such existing data. BA shall record any modification of data and retain such record for a period of seven (7) years.

2.12 Disclosure of Practices, Books and Records. Unless otherwise protected from discovery or disclosure by law, BA agrees to make its internal practices, books, and records relating to the use or disclosure of PHI received from, or created or received by BA on behalf of the CE, available to the Secretary or designee for purposes of determining compliance with applicable laws and agency guidance.

2.13 Make Available Information for Accounting of Disclosures. Twenty (20) calendar days after receipt of written notice from CE that CE needs to provide an Individual with an accounting of disclosures of PHI in accordance with 45 CFR

§164.528, BA agrees to make available to CE information concerning disclosure of PHI by BA or its agents. To the extent required of BA under Section 13405(c) of the HITECH Act, if CE uses or maintains EHR, BA will include in the accounting disclosures made for treatment, payment, or health care operations purposes through the EHR. BA agrees to make available to the Individual the information described above if properly requested by the subject Individual. Should an accounting of the PHI of a particular Individual be requested more than once in any twelve month period, BA may charge a reasonable, cost-based fee. BA shall have a reasonable time within which to comply with such requests and, in no case, shall access be required in less than twenty (20) calendar days after BA's receipt of such request.

2.14 Restrict Disclosure of PHI. Upon written request by CE on behalf of an Individual, BA agrees to consider restrictions on the use or disclosure of PHI requested by CE. BA will grant requests to limit disclosures to health plans for payment or health care operations purposes when the provider has been paid out of pocket in full for services or products as provided in Section 13405(a) of the HITECH Act.

2.15 Restrict exchange of PHI with violators. BA will refrain from exchanging any PHI with any entity that the BA knows has a pattern of activity or practice that constitutes a material breach or violation of HIPAA.

2.16 Use of PHI as Permitted by Authorizations. Notwithstanding any other limitation in Section 2 of this agreement, BA and CE agree that nothing in this Agreement prohibits BA from using or disclosing PHI to the extent permitted by an authorization from the appropriate Individual.

2.17 Additional Obligations Imposed by the HITECH Act. BA agrees to abide by all the following to the extent they are implicated by the Underlying Agreement with CE:

a) BA will not disclose PHI to a health plan if the Individual to whom the PHI pertains has so requested and (1) the disclosure would be for the purposes of payment or health care operations, and not for the purposes of treatment, (2) the protected health information at issue pertains to a health care item or service for which the Individual pays out-of-pocket and in full, and (3) the disclosure is not required by law.

b) BA agrees to comply with all privacy laws governing marketing communications, that is, communications about a product or service that encourages the recipient to purchase or use the product or service.

c) BA agrees to clearly and conspicuously provide any recipient of health care fundraising communications the opportunity to opt out of receiving any further such solicitations.

d) BA understands and agrees that it will be subject to the same penalties as a Covered Entity for any violation of the HIPAA Security requirements and for violations of the Privacy Rule for impermissible uses and disclosures, for a failure to provide breach notification to the covered entity, for a failure to provide access to a copy of electronic protected health information to the covered entity, for a failure to disclose protected health information where required by the Secretary to investigate or determine Business Associate's compliance with the HIPAA Rules, and for a failure to provide an accounting of disclosures, and that it will be subject to periodic audits by HHS. BA further understands and agrees that any of its agents and subcontractors will be held to the same standards and that such provision will be incorporated into any BA agreement with said agents and subcontractors.

e) BA agrees to comply with all privacy laws governing the sale of PHI.

SECTION 3: PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

3.1 Use of PHI for Specific Purposes. Except as otherwise provided in this Agreement, BA may use, request or disclose only the minimum necessary PHI in order to perform specific functions, activities, or services for, or on behalf of, CE as specified by CE, provided that such use or disclosure would not violate the HIPAA Regulations or the HITECH Act and the Privacy Rule if done by CE or the minimum necessary policies and procedures of the CE, except as provided herein. BA may make such uses and disclosures of PHI as are reasonably necessary to perform its contractual and legal obligations to CE under this agreement, or as otherwise required by law. Such uses and disclosures include, but are not limited to, disclosures to records production and copying vendors, disclosures to employees or other agents of BA, and use as evidence in connection with court or other legal proceedings, or as otherwise permitted by law. All other uses not authorized by this Agreement or by law are prohibited.

3.2 Disclosure of PHI for Administration and Legal Responsibilities. Except as otherwise provided in this Agreement, BA may use PHI for the proper management and administration of BA or to carry out the legal responsibilities of BA. Except as otherwise provided in this Agreement, BA may disclose PHI for the proper management and administration of BA or to carry out the legal responsibilities of BA provided that i) such disclosures are required by law; or ii) BA obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies BA of any instances of which it is aware in which the confidentiality of the information has been breached.

3.3 Disclosure of PHI to Report Violations of the Law. BA may disclose PHI to report violations of the law to law enforcement.

3.4 De-Identification. BA may use PHI to create de-identified information consistent with the standards set forth at 45 CFR §164.514.

SECTION 4: OBLIGATIONS OF COVERED ENTITY

CE shall notify BA of any limitation(s) on use or disclosure based on CE's notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect BA's use or disclosure of PHI. CE shall notify BA 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. CE shall notify BA of any restriction on the use or disclosure of PHI that CE has agreed to in accordance with 45 CFR §164.522, to the extent such restriction may affect BA's use or disclosure of PHI.

SECTION 5: IMPERMISSIBLE REQUESTS BY COVERED ENTITY

CE shall not ask BA to use or disclose PHI in any manner that would not be permissible under the HIPAA Regulations or HITECH Standards if done by CE. However, BA may use or disclose PHI for management and administrative activities of BA, as is otherwise permitted by this Agreement, or as is required or permitted by law.

SECTION 6: TERMINATION

6.1 Term and Disposition of PHI. This Agreement shall be effective during the term of the services rendered by BA to CE or until otherwise terminated by BA and CE, or when all of the PHI provided by CE to BA, or created or received by BA on CE's behalf, is destroyed or returned to CE; or, if it is not feasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this section. BA shall extend the protections of this Agreement to such PHI and shall limit further uses and disclosures of such PHI, for so long as the BA maintains such PHI. Notwithstanding any other limitation in this section, BA agrees that it is not necessary to return or destroy PHI received from, or created or received by BA on behalf of CE, if patient authorizations permitting such retention have been executed. Any destruction of PHI will be done in a manner so as to render the PHI unidentifiable.

6.2 Termination for Cause. Upon either party's knowledge of a violation of a material term of this Agreement by the other party, the non-violating party shall provide an opportunity for the other party to cure the breach or end the violation. The non-violating party may terminate this Agreement if the violating party has violated a material term of the Agreement and cure is not possible. If a cure is not effectuated within a reasonable time period specified by the party requesting the cure following the date of discovery, such party shall terminate the Agreement if feasible, or if termination is not feasible, report the problem to the Secretary.

SECTION 7: GENERAL PROVISIONS

7.1 Regulatory References. A reference in this Agreement to a Section in the HIPAA Regulations or HITECH Standards means the Section in effect or as amended, and with which compliance is required.

7.2 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits compliance with the HIPAA Regulations and HITECH Standards.

7.3 Enforceability. If any provision of this Agreement is held invalid or unenforceable, such invalidity or unenforceability shall apply only to such provision and shall not in any way affect or render invalid or unenforceable any other provision of this Agreement.

7.4 Survival. The rights and obligations of BA under this Agreement survive the termination of this Agreement.

7.5 Amendment. BA or CE, at its discretion, may amend this Agreement from time to time, to comply with HIPAA, the HITECH Act, amendments that may be made to them, regulations, or other federal laws that may be promulgated and affect the provisions of this Agreement.

7.6 Choice of Law. This Agreement is made in and will be governed by, and construed in accordance with, the laws of the state in which the CE is insured by BA without regard to principles of conflict or choice of law.

7.7 Communications. All notices or communications required or permitted pursuant to the terms of this Agreement shall be in writing. All such notices will be effective immediately upon delivery in person, on the third business day after deposit with the U.S. Postal Service, or on the first business day after sending by facsimile or email. Notices shall be sent to the following addresses, phone numbers and/or email addresses:

Andrew Firth, President

Business Associate:

MEDICAL INSURANCE EXCHANGE OF CALIFORNIA
6250 Claremont Avenue
Oakland, CA 94618

Phone: 510/428-9411
Fax: 510/654-4634