HIPAA

NORCAL BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA") is entered into by and between NORCAL Mutual Insurance Company ("NORCAL") and Insured/Applicant ("Covered Entity") and is effective as of September 23rd, 2013 (the "BAA Effective Date"). NORCAL and Covered Entity may be referred to individually as a "Party" or, collectively, as the "Parties" in this BAA.

RECITALS

1. NORCAL and Covered Entity have an insurer/insured relationship by virtue of a professional liability policy (the "Policy") requested from or issued by NORCAL. NORCAL and its insureds and applicants are committed to protecting the privacy and providing for the security of Protected Health Information (as that term is defined below) disclosed to NORCAL pursuant to the Policy in compliance with (i) the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); (ii) Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), also known as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 ("ARRA"); and (iii) regulations promulgated thereunder by the U.S. Department of Health and Human Services, including the HIPAA Omnibus Final Rule (the "HIPAA Final Rule"), which amended the Privacy Rule and the Security Rule (as those terms are defined below) pursuant to the HITECH Act, extending certain HIPAA obligations to business associates and their subcontractors.

2. The purpose of this BAA is to satisfy certain standards and requirements of HIPAA, the Privacy Rule and the Security Rule (as those terms are defined below), and the HIPAA Final Rule, including, but not limited to, Title 45, §§ 164.314(a)(2)(i), 164.502(e) and 164.504(e) of the Code of Federal Regulations ("C.F.R.").

In consideration of the mutual promises below and the exchange of information pursuant to this BAA, the Parties agree as follows:

1. DEFINITIONS

a. **Capitalized Terms.** Capitalized terms used in this BAA and not otherwise defined herein shall have the meanings set forth in the Privacy Rule, the Security Rule and the HIPAA Final Rule, which definitions are incorporated in this BAA by reference.

b. **"Breach"** shall have the same meaning given to such term in 45 C.F.R. § 164.402.

c. **"Designated Record Set"** shall have the same meaning given to such term in 45 C.F.R. § 164.501.

d. **"Electronic Protected Health Information" or "Electronic PHI"** 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. § 160.103, as applied to the information that NORCAL creates, receives, maintains or transmits from or on behalf of Covered Entity.

e. **"Individual"** shall have the same meaning as the term "individual" in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

f. **"Privacy Rule"** shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

g. **"Protected Health Information" or "PHI"** shall have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, as applied to the information created, received, maintained or transmitted by NORCAL from or on behalf of Covered Entity.

h. **"Required by Law"** shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

i. **"Secretary"** shall mean the Secretary of the Department of Health and Human Services or his or her designee.

j. **"Security Incident"** shall have the meaning given to such term in 45 C.F.R. § 164.304.

k. **"Security Rule"** shall mean the Security Standards at 45 C.F.R. Part 160 and Part 164, Subparts A and C.

l. **"Unsecured PHI"** shall have the same meaning given to such term under 45 C.F.R. § 164.402, and guidance promulgated thereunder.

2. PERMITTED USES AND DISCLOSURES OF PHI

a. **Uses and Disclosures of PHI Pursuant to Policy.** Under the Policy, NORCAL provides Covered Entity with insurance products and services (the "Services") that involve the use and disclosure of PHI. The Services may include: (i) the acceptance, declination or acceptance with revisions of professional liability insurance; (ii) receiving and evaluating incidents, claims and lawsuits; (iii) quality assessment; (iv) quality improvement; (v) loss prevention tools; (vi) outcomes evaluation; (vii) protocol and clinical guidelines development; (viii) reviewing the competence or qualifications of health care professionals; (ix) evaluating practitioner and provider performance; (x) conducting training programs to improve the skills of health care practitioners and providers; (xi) credentialing, conducting or arranging for medical review; (xii) arranging for legal services; (xiii) conducting or arranging for audits to improve compliance; (xiv) resolution of internal grievances; (xv) placing insurance or reinsurance, including, but not limited to, pro rata stop-loss and excess-of-loss insurance and (xvi) other functions necessary to

perform the Services. Except as otherwise limited in this BAA, NORCAL may use or disclose PHI to perform the Services for or on behalf of, Covered Entity, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity. To the extent NORCAL is carrying out one or more of Covered Entity's obligations under the Privacy Rule pursuant to the terms of the Policy or this BAA, NORCAL shall comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligation(s).

b. **Permitted Uses of PHI by NORCAL.** Except as otherwise limited in this BAA, NORCAL may use PHI for the proper management and administration of NORCAL or to carry out the legal responsibilities of NORCAL.

c. **Permitted Disclosures of PHI by NORCAL.** Except as otherwise limited in this BAA, NORCAL may disclose PHI for the proper management and administration of NORCAL, provided that the disclosures are Required by Law, or NORCAL 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 (which purpose must be consistent with the limitations imposed upon NORCAL pursuant to this BAA), and that the person agrees to notify NORCAL of any instances of which it is aware in which the confidentiality of the information has been breached. NORCAL may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1).

d. **Data Aggregation.** Except as otherwise limited in this BAA, NORCAL may use PHI to provide Data Aggregation services as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

e. **De-identified Data.** NORCAL may create de-identified PHI in accordance with the standards set forth in 45 C.F.R. § 164.514(b) and may use or disclose such de-identified data for any purpose.

3. OBLIGATIONS OF NORCAL

a. **Appropriate Safeguards.** NORCAL shall use appropriate safeguards and shall, after the compliance date of the HIPAA Final Rule, comply with the Security Rule with respect to Electronic PHI, to prevent use or disclosure of such information other than as provided for in this BAA.

b. **Reporting of Improper Use or Disclosure, Security Incident or Breach.** NORCAL shall report to Covered Entity any use or disclosure of PHI not permitted under this BAA, Breach of Unsecured PHI or Security Incident, without unreasonable delay, and in any event no more than thirty (30) days following discovery; provided, however, that the Parties acknowledge and agree that this Section constitutes notice by NORCAL to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which notice to Covered Entity by NORCAL shall be required only upon request. "Unsuccessful Security Incidents" shall include, but not be limited to, pings and other broadcast attacks on NORCAL's firewall, port scans, unsuccessful

log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI. NORCAL's notification to Covered Entity of a Breach shall include: (i) the identification of each individual whose Unsecured PHI has been, or is reasonably believed by NORCAL to have been, accessed, acquired or disclosed during the Breach; and (ii) any particulars regarding the Breach that Covered Entity would need to include in its notification, as such particulars are identified in 45 C.F.R. § 164.404

c. **NORCAL's Agents.** In accordance with 45 C.F.R. § 164.502(e)(1)(ii) and 45 C.F.R. § 164.308(b)(2), as applicable, NORCAL shall enter into a written agreement with any agent or subcontractor that creates, receives, maintains or transmits PHI on behalf of NORCAL for services provided to Covered Entity, providing that the agent agrees to restrictions and conditions that are substantially similar to those that apply through this BAA to NORCAL with respect to such PHI.

d. **Access to PHI.** The Parties do not intend for NORCAL to maintain any PHI in a Designated Record Set for Covered Entity. To the extent NORCAL possesses PHI in a Designated Record Set, NORCAL agrees to make such information available to Covered Entity pursuant to 45 C.F.R. § 164.524 within ten (10) business days of NORCAL's receipt of a written request from Covered Entity. If an Individual makes a request for access pursuant to 45 C.F.R. § 164.524 directly to NORCAL, or inquires about his or her right to access, NORCAL shall direct the Individual to Covered Entity.

e. **Amendment of PHI.** The Parties do not intend for NORCAL to maintain any PHI in a Designated Record Set for Covered Entity. To the extent NORCAL possesses PHI in a Designated Record Set, NORCAL agrees to make such information available to Covered Entity for amendment pursuant to 45 C.F.R. § 164.526 within twenty (20) business days of NORCAL's receipt of a written request from Covered Entity. If an Individual submits a written request for amendment pursuant to 45 C.F.R. § 164.526 directly to NORCAL, or inquires about his or her right to amendment, NORCAL shall direct the Individual to Covered Entity.

f. **Documentation of Disclosures.** NORCAL agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. NORCAL shall document, at a minimum, the following information ("Disclosure Information"): (i) the date of the disclosure; (ii) the name and, if known, the address of the recipient of the PHI; (iii) a brief description of the PHI disclosed; (iv) the purpose of the disclosure that includes an explanation of the basis for such disclosure; and (v) any additional information required under the HITECH Act and any implementing regulations.

g. **Accounting of Disclosures.** NORCAL agrees to provide to Covered Entity, within twenty (20) business days of NORCAL's receipt of a written request from Covered Entity, information collected in accordance with Section 3(f) of this BAA, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. If an Individual submits a written request for an accounting of disclosures pursuant to 45 C.F.R. § 164.528 directly to NORCAL, or inquires about his or her right to an accounting of disclosures, NORCAL shall direct the Individual to Covered Entity.

h. **Governmental Access to Records.** NORCAL shall make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by NORCAL on behalf of, Covered Entity available to the Secretary for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

i. **Mitigation.** To the extent practicable, NORCAL will reasonably cooperate with Covered Entity's efforts to mitigate a harmful effect that is known to NORCAL of a use or disclosure of PHI that is not permitted by this BAA.

j. **Minimum Necessary.** NORCAL shall request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure, in accordance with 45 C.F.R. § 164.514(d), and any amendments thereto.

k. **HIPAA Final Rule Applicability.** NORCAL acknowledges that enactment of the HITECH Act, as implemented by the HIPAA Final Rule, amended certain provisions of HIPAA in ways that now directly regulate, or will on future dates directly regulate, NORCAL under the Privacy Rule and the Security Rule. NORCAL agrees, as of the compliance date of the HIPAA Final Rule, to comply with applicable requirements imposed under the HIPAA Final Rule.

4. OBLIGATIONS OF COVERED ENTITY

a. **Notice of Privacy Practices.** Covered Entity shall notify NORCAL of any limitation(s) its notice of privacy practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect NORCAL's use or disclosure of PHI. Covered Entity shall provide such notice no later than fifteen (15) days prior to the effective date of the limitation.

b. **Notification of Changes Regarding Individual Permission.** Covered Entity shall notify NORCAL of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect NORCAL's use or disclosure of PHI. Covered Entity shall provide such notice no later than fifteen (15) days prior to the effective date of the change. Covered Entity shall obtain any consent or authorization that may be required by the HIPAA Privacy Rule, or applicable state law, prior to furnishing NORCAL with PHI.

c. **Notification of Restrictions to Use or Disclosure of PHI.** Covered Entity shall notify NORCAL of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect NORCAL's use or disclosure of PHI. Covered Entity shall provide such notice no later than fifteen (15) days prior to the effective date of the restriction. If NORCAL reasonably believes that any restriction agreed to by Covered Entity pursuant to this Section may materially impair NORCAL's ability to perform its obligations under the Underlying Agreement or this BAA, the Parties shall mutually agree upon any necessary modification of NORCAL's obligations under such agreements.

d. **Permissible Requests by Covered Entity.** Covered Entity shall not request NORCAL to use or disclose PHI in any manner that would not be permissible under the Privacy Rule, the Security Rule or the HIPAA Final Rule if done by Covered Entity, except as permitted pursuant to the provisions of Section 2 of this BAA.

5. TERM AND TERMINATION

a. **Term.** The term of this BAA shall commence as of the BAA Effective Date, and shall terminate when all of the PHI provided by Covered Entity to NORCAL, or created or received by NORCAL on behalf of Covered Entity, is destroyed or returned to Covered Entity or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with Section 5(c).

b. **Termination for Cause.** Upon either Party's knowledge of a material breach by the other Party of this BAA, such Party shall provide written notice to the breaching Party detailing the nature of the breach and providing an opportunity to cure the breach within thirty (30) business days. Upon the expiration of such 30-day cure period, the non-breaching Party may terminate this BAA if cure is not possible.

c. **Effect of Termination.**

(i) Except as provided in paragraph (ii) of this Section 5(c), upon termination of this BAA for any reason, NORCAL shall return or destroy all PHI received from Covered Entity, or created or received by NORCAL on behalf of Covered Entity, and shall retain no copies of the PHI. This provision shall apply to PHI that is in the possession of subcontractors or agents of NORCAL.

(ii) Upon termination of NORCAL's provision of Services under the Policy, NORCAL agrees to return or destroy all PHI, pursuant to 45 C.F.R. § 164.504(e)(2)(ii)(J), to the extent that it is feasible to do so, and to require any and all of its subcontractors or agents to return or destroy any PHI in their possession. However, NORCAL and Covered Entity hereby acknowledge and agree that, due to the nature of the Services provided by NORCAL and its business obligations, it is not feasible to return or destroy all PHI immediately on termination of this BAA, or for some time thereafter. Therefore, NORCAL agrees to extend, and require its subcontractor and agents to

extend, the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make return or destruction infeasible, for so long as NORCAL maintains such PHI. This Section 5(c)(ii) shall survive termination of this BAA and NORCAL's provision of Services under the Policy.

6. COOPERATION IN INVESTIGATIONS

The Parties acknowledge that certain breaches or violations of this BAA may result in litigation or investigations pursued by federal or state governmental authorities of the United States resulting in civil liability or criminal penalties. Each Party shall cooperate in good faith in all respects with the other Party in connection with any request by a federal or state governmental authority for additional information and documents or any governmental investigation, complaint, action or other inquiry.

7. REGULATORY REFERENCES

A reference in this BAA to a section in the Privacy Rule, the Security Rule or the HIPAA Final Rule means the section as in effect or as amended, and for which Covered Entity's and/or NORCAL's compliance is required.

8. AMENDMENT

If any relevant provision of the Privacy Rule, the Security Rule or the HIPAA Final Rule is amended in a manner that changes the obligations of NORCAL or Covered Entity that are embodied in terms of this BAA, then the Parties agree to negotiate in good faith appropriate non-financial terms or amendments to this BAA to give effect to such revised obligations.

9. NO THIRD PARTY BENEFICIARIES

Nothing express or implied in this BAA is intended to confer upon any person other than Covered Entity, NORCAL and their respective successors and assigns, any rights, remedies or liabilities whatsoever.

10. GENERAL

This BAA is governed by, and shall be construed in accordance with, the laws of the State that govern the Policy. Covered Entity shall not assign this BAA without the prior written consent of NORCAL, which shall not be unreasonably withheld. If any part of a provision of this BAA is found illegal or unenforceable, it shall be enforced to the maximum extent permissible, and the legality and enforceability of the remainder of that provision and all other provisions of this BAA shall not be affected. All notices relating to the Parties' legal rights and remedies under this BAA shall be provided in writing to a Party, and shall be sent to the address in the Policy contract of the Insured/Applicant, or to the last known address of the Insured/Applicant or to such other address as may be designated by that Party by notice to the sending Party, and shall reference this BAA. This BAA may be modified, or any rights under it waived, only by a written document executed by the authorized representatives of both Parties. This BAA is the complete and exclusive agreement between the Parties with respect to the subject matter hereof, superseding and replacing all prior agreements, communications and understandings (written and oral) regarding its subject matter.

Scott Diener
President

Kara M. Ricci
Secretary