KAISER PERMANENTE

Kaiser Permanente® Business Associate Agreement

THIS BUSINESS ASSOCIATE AGREEMENT ("BAA") SHALL APPLY TO ANY SUPPLIER THAT HAS A BUSINESS RELATIONSHIP (AS DEFINED BELOW) WITH A COVERED ENTITY AS DEFINED BELOW THAT INVOLVES THE RECEIPT, CREATION, MAINTENANCE, ACCESS, TRANSMISSION, USE AND/OR DISCLOSURE OF PHI (AS DEFINED BELOW) TO THE EXTENT THE SUPPLIER QUALIFIES AS A BUSINESS ASSOCIATE UNDER HIPAA REGULATIONS. THIS AGREEMENT APPLIES UNLESS SUPPLIER AND COVERED ENTITY HAVE A SEPARATELY SIGNED BUSINESS ASSOCIATE AGREEMENT.

In order to protect the privacy of the PHI and to comply with HIPAA and the HIPAA Regulations (as defined below), Covered Entity and Business Associate desire to enter into this BAA setting forth the terms and conditions of the use and disclosure of PHI pursuant to one or more agreement(s) under which Business Associate provides or will provide certain specified services to Covered Entity (the "Business Relationship").

In consideration of the mutual promises set forth below, the parties agree as follows:

1. DEFINITIONS

1.1 General Rule. Capitalized terms not otherwise defined in this BAA shall have the same meaning as those terms in the Privacy Rule, the Security Rule, the Breach Notification Rule, and in HIPAA and the HITECH Act, and any regulations promulgated thereunder, as and when amended from time to time.

1.2 "Breach" shall have the meaning provided under 45 C.F.R. Section 164.402, as and when amended from time to time.

1.3 "Breach Notification Rule" means the Breach Notification for Unsecured Protected health Information interim Final Rule at 45 C.F.R. Parts 160 and 164, Subpart D, as and when amended from time to time.

1.4 "Covered Entity" or "Covered Entities" means (i) the Covered Entities participating in the integrated health care delivery system doing business as Kaiser Permanente®, including Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, the Permanente Medical Groups, and all subsidiaries and successors of the foregoing, and (ii) Risant Health, Inc. and Kaiser Permanente Insurance Company, and all subsidiaries and successors of the foregoing.

1.5 "Electronic Health Record" shall have the meaning provided under Section 13400(5) of the HITECH Act (42 U.S.C. Section 17921(5)), as and when amended from time to time.

1.6 "EPHI" means electronic protected health information as defined in 45 C.F.R. Section 160.103, as and when amended from time to time.

1.7 "HIPAA" means the Health Insurance Portability & Accountability Act of 1996, P.L. 104-191 as and when amended from time to time.

1.8 "HIPAA Regulations" means the regulations promulgated under HIPAA and the HITECH Act by the U.S. Department of Health and Human Services ("HHS"), including, but not limited to the Privacy Rule, the Security Rule and the Breach Notification Rule, as and when amended from time to time.

1.9 "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, as and when amended from time to time.

1.10 "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information, codified at 45 C.F.R. parts 160 and 164, Subparts A and E, as amended from time to time.

1.11 "PHI" means Protected Health Information, as that term is defined under the Privacy Rule, including but not limited to, 45 C.F.R. Section 160.103, that is provided by a Covered Entity to Business Associate, or is created, received, transmitted or maintained by Business Associate on behalf of a Covered Entity.

1.12 "Secretary" means the Secretary of HHS.

1.13 "Security Rule" means the Standards for Security for the Protection of Electronic Protected Health Information, codified at 45 C.F.R. parts 160 and 164, Subpart C, as amended from time to time.

1.14 "Substance Use Disorder Records" means any records, whether paper or electronic, which were created, received or acquired by a federally assisted program that is subject to 42 C.F.R. Part 2 and which relate to a patient (e.g., diagnosis, treatment and referral for treatment information; billing information; emails, voice mails and texts), as such terms are defined in 42 C.F.R. Part 2.

1.15 "Unsecured Protected Health Information" shall have the meaning provided under 45 C.F.R. Section 164.402, as amended from time to time.

2. OBLIGATIONS OF BUSINESS ASSOCIATE

2.1 General Requirements. Except as otherwise limited in this BAA, Business Associate may Use or Disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entities under the terms of the Business Relationship, subject to any limitations described herein, and provided that such Use or Disclosure would not violate the Privacy Rule if done by Covered Entities. Business Associate shall limit its Use, Disclosure or request of PHI, to the extent practicable, to a Limited Data Set or, if needed by Business Associate, to the Minimum Necessary amount of PHI needed to accomplish the intended purpose of the Use, Disclosure or request, in accordance with any guidance issued by HHS. Business Associate shall comply with all applicable provisions of HIPAA, the HITECH Act and the HIPAA Regulations, and shall not Use or Disclose PHI other than as permitted by this BAA or as required by law.

2.2 Uses Permitted By Law. To the extent permitted by law, including, without limitation, the Privacy Rule, Business Associate may (a) Use PHI as is necessary for the proper management and administration of Business Associate's organization, or to carry out the legal responsibilities of Business Associate; and (b) Disclose PHI for the purposes described in subsection 2.2(a) above, provided that (i) the Disclosure is required by law or (ii) Business Associate obtains reasonable assurances from the recipient of the information that the information will be held confidentially and Used or further Disclosed only as required by law or for the purpose for which it was Disclosed to the person, and the recipient notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

2.3 Data Aggregation and Data Use Restrictions. Business Associate may not perform Data Aggregation services, unless relating to the Health Care Operations of Covered Entities if required by Covered Entities under the Business Relationship. Additionally, Business Associate is prohibited from de-identifying (or reidentifying), selling, distributing, commercially exploiting, aggregating (except with respect to Data Aggregation services if the exception in the foregoing sentence applies), data mining, analyzing, benchmarking or otherwise using or disclosing any PHI (including any anonymized, de-identified (or reidentified) or aggregated PHI) for any purpose except as required to provide the services to Covered Entities under the Business Relationship.

2.4 Disclosures to Subcontractors. Business Associate shall ensure that any Subcontractor of Business Associate that creates, receives, maintains or transmits PHI agrees in writing to the same restrictions and conditions that apply to Business Associate regarding the Use and Disclosure and security of PHI. Business Associate shall not permit any Subcontractor that fails to abide by any material term of such agreement to create, receive, maintain, transmit, or otherwise Use or Disclose PHI.

2.5 Safeguards. Business Associate shall implement and use appropriate safeguards as necessary to prevent the Use or Disclosure of PHI in any manner that is not permitted by this BAA, as required by the Privacy Rule.

2.6 Mitigation. Business Associate shall mitigate promptly, to the extent practicable, any harmful effect (a) that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of this BAA, the Privacy Rule, or other applicable federal or state law or (b) of a Security Incident for which Business Associate is responsible, or of which Business Associate is aware, that involves EPHI and is in violation of this BAA, the Security Rule, or other applicable federal or state law.

2.7 Access and Amendment. To enable Covered Entities to fulfill their obligations under 45 C.F.R. Sections 164.524 and 164.526, Business Associate shall make PHI in Designated Record Sets that are maintained by Business Associate or its Subcontractors available to Covered Entities for inspection, copying or amendment within ten (10) calendar days of a request by Covered Entities. If PHI is maintained in an electronic Designated Record Set, then Business Associate shall provide Covered Entities with a copy of such information in electronic format in accordance with 45 C.F.R. Section 164.524 within ten (10) calendar days of a request by Covered Entities. If an Individual requests inspection, copying or amendment of PHI directly from Business Associate or its Subcontractors, Business Associate shall notify Covered Entities in writing within five (5) business days of Business Associate's receipt of the request, and shall defer to, and comply with, Covered Entities' direction in a timely manner regarding the response to the Individual regarding the request for inspection, copying or amendment.

2.8 Accounting. Business Associate shall record and make available to Covered Entities Covered Disclosures of PHI by Business Associate ("Accounting Information") as necessary to enable Covered Entities to comply timely with their obligations under the Privacy Rule including, but not limited to, 45 C.F.R. Section 164.528. For purposes of this BAA, "Covered Disclosure" means any Disclosure of PHI subject to the Individual's right under the HIPAA Regulations to an accounting of such Disclosures. At a minimum, this Accounting Information shall include for each such Disclosure the information required by 45 C.F.R. Section 164.528(b). Within ten (10) calendar days of notice from Covered Entities of a request for an accounting of Disclosures of PHI, Business Associate shall make available to Covered Entities this Accounting Information. If an Individual requests an accounting directly from Business Associate or its Subcontractors, Business Associate must notify Covered Entities in writing within five (5) business days of the request, and shall defer to, and comply in a timely manner with, Covered Entities' direction regarding the response to the Individual regarding the request for an accounting. In addition, as of the effective date of Section 13405(c) of the HITECH Act (42 U.S.C. Section 17935(c)), to the extent Business Associate is using or maintaining an Electronic Health Record, Business Associate shall provide to Covered Entities, or, at Covered Entities' request, to an Individual, an accounting of Disclosures to carry out Treatment, Payment or Health Care Operations through the Electronic Health Record made by Business Associate for the three (3) years prior to the request, unless such an accounting would be otherwise excepted by Section 13405 of the HITECH Act, implementing regulations, or guidance issued from HHS. Such accounting of routine Disclosures shall be in a form that is compliant with any regulations or guidance issued by the Secretary.

2.9 Government Officials. Business Associate shall make its internal practices, books and records relating to the Use and Disclosure of PHI available to the Secretary for purposes of determining Covered Entities' compliance with the Privacy Rule. Business Associate shall notify Covered Entities regarding any PHI that Business Associate provides to the Secretary concurrently with providing such PHI to the Secretary, and upon Covered Entities' request, shall provide Covered Entities with a duplicate copy of such PHI.

2.10 Insurance and Indemnity.

2.10.1 Business Associate shall maintain or cause to be maintained sufficient insurance coverage as shall be necessary to insure Business Associate and its Subcontractors against any claim or claims for damages arising under this BAA including maintaining cyber liability insurance that complies with Covered Entities' Insurance Requirements posted on Covered Entities' website: http://supplier.kp.org/formsreqs/index.html. Such insurance coverage shall apply to all site(s) of Business Associate and to all services provided by Business Associate or its Subcontractors under this BAA. This provision shall govern the Business Associate's insurance and indemnity obligations, unless the Business Relationship between the Business Associate and Covered Entities provides for additional and more explicit requirements.

2.10.2 Business Associate shall indemnify, hold harmless and defend Covered Entities from and against any and all claims, losses, liabilities, costs and other expenses (including reasonable attorneys' fees and costs, and administrative penalties and fines) incurred as a result of, or arising directly or indirectly out of or in connection with any act or omission of Business Associate, its Subcontractors, under this BAA including, but not limited to, negligent or

intentional acts or omissions. The indemnification obligation of Business Associate shall survive termination of this BAA.

2.11 Compliance with the Security Rule. To the extent that Business Associate creates, receives, maintains, or transmits EPHI, Business Associate shall comply with the provisions of the Security Rule, including, without limitation, implementing administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any EPHI that Business Associate may create, receive, maintain or transmit on behalf of Covered Entities; implementing policies and procedures; and complying with documentation requirements.

2.12 Reporting of Security Incidents. If the Business Associate creates, receives, maintains, or transmits EPHI, Business Associate shall appropriately report any Security Incident to Covered Entities; provided, however, that any security incident that is a Breach of Unsecured Protected Health Information shall be reported pursuant to Section 2.13. This Section constitutes notice by Business Associate to Covered Entities of the ongoing occurrence of attempted Unsuccessful Security Incidents for which no additional notice to Covered Entities shall be required. "Unsuccessful Security Incidents" means pings and other broadcast attacks or reconnaissance scans on Business Associate's firewall, port scans, unsuccessful log-on attempts, and any combination of the above, so long as no such incident results in any Breach of EPHI or access, Use or Disclosure of EPHI in violation of this BAA.

2.13 Reporting of Breaches of Unsecured Protected Health Information. Business Associate, following the discovery of a Breach of Unsecured Protected Health Information, subject to any law enforcement delay permitted by 45 C.F.R. Section 164.412, shall notify Covered Entities of the Breach immediately, but in no event later than five (5) calendar days thereafter (unless a shorter period for notification is required by your Business Relationship with Covered Entities), by calling the Kaiser Permanente National Compliance Hotline at 1-888-774-9100 and providing notice as set forth in Section 5.8 (Notices) below. A Breach shall be treated as discovered by the Business Associate pursuant to the provisions of 45 C.F.R. Section 164.410(a)(2). The information included in Business Associate's notification shall be in accordance with the HIPAA Regulations, including, without limitation, 45 C.F.R. Section 164.410(c), and guidance provided by the Secretary.

2.14 Notices of Prohibited Uses or Disclosures. Except in the case of a Breach of Unsecured Protected Health Information, which shall be governed by the provisions of Section 2.13, Business Associate shall provide written notice to Covered Entities of any Use or Disclosure of PHI that is in violation of this BAA, the Privacy Rule, or other applicable federal or state law within five (5) business days of becoming aware of such Use or Disclosure. Business Associate shall also notify Covered Entities in writing within five (5) business days of receipt of any complaint that Business Associate receives concerning the handling of PHI or compliance with this BAA.

2.15 Delegated Activities. To the extent that Business Associate is to carry out one or more of Covered Entities' obligations under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to Covered Entities in the performance of such obligations.

2.16 Substance Use Disorder Records. If Business Associate receives Substance Use Disorder Records from a Covered Entity: (i) Business Associate may use and disclose those records in accordance with this BAA, except that such records may not be used or disclosed for civil, criminal, administrative or legislative proceedings against the Individual who is the subject of the Substance Use Disorder Records unless required pursuant to a court order issued under 42 C.F.R. Part 2, Subpart E; and (ii) If Business Associate qualifies as a qualified service organization of a Covered Entity's part 2 program as defined in 42 C.F.R. Section 2.11, Business Associate acknowledges that in receiving, storing, processing, or otherwise dealing with any Substance Use Disorder Records from the part 2 program, it is fully bound by the regulations in 42 C.F.R. Part 2 (in addition to the requirements of this BAA), and if necessary, will resist in judicial proceedings any efforts to obtain access to patient identifying information related to substance use disorder diagnosis, treatment, or referral for treatment except as permitted by 42 C.F.R., Part 2.

3. OBLIGATIONS OF COVERED ENTITIES

3.1. Notice of Privacy Practices. Covered Entities shall notify Business Associate of limitation(s) in its

notice of privacy practices in accordance with 45 C.F.R. Section 164.520, to the extent such limitation affects Business Associate's permitted Uses or Disclosures.

3.2. Individual Permission. Covered Entities shall notify Business Associate of changes in, or revocation of, permission by an Individual to Use or Disclose PHI, to the extent such changes affect Business Associate's permitted Uses or Disclosures.

3.3. Restrictions. Covered Entities shall notify Business Associate of restriction(s) in the Use or Disclosure of PHI requested by an Individual and to which Covered Entities have agreed or with which Covered Entities are required to comply in accordance with 45 C.F.R. Section 164.522, to the extent such restriction affects Business Associate's permitted Uses or Disclosures.

3.4. Prohibited Requests. Covered Entities shall not request Business Associate to Use or Disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entities.

4. TERM AND TERMINATION

4.1. Term. This BAA shall commence as of the start of the Business Relationship and shall continue in effect unless and until the earlier of the termination of the Business Relationship between Covered Entities and Business Associate or termination by Covered Entities under this Section 4.1 or Section 4.2. Covered Entities may terminate this BAA, without cause, on five (5) calendar days' prior written notice to Business Associate. To the extent that such termination of this BAA without cause necessarily results in a termination of the Business Relationship between the parties, the termination of such Business Relationship shall be subject to any requirements of the Business Relationship with respect to a termination without cause.

4.2. Termination for Cause by Covered Entities. If Covered Entities determine that Business Associate, or any of its Subcontractors, has breached any material provision of this BAA, which may include a pattern of activity or practice that constitutes a material breach, then Covered Entities, in their sole discretion, may (a) notify Business Associate of the material breach and request that it be cured or (b) if feasible, terminate this BAA and Covered Entities' Business Relationship with Business Associate immediately or upon such notice as Covered Entities may determine. If Covered Entities notify Business Associate of the material breach and requests that it be cured under (a) above, and Business Associate fails to cure the material breach to the reasonable satisfaction of Covered Entities, then Covered Entities may, in their sole discretion, terminate this BAA and Covered Entities' Business Relationship with Business Associate immediately or upon such notice as Covered Entities may determine.

4.3. Effects of Termination. Upon termination of the Business Relationship between the parties and/or the BAA for any reason, Business Associate shall, at Covered Entities' direction, return or destroy all PHI (including, without limitation, EPHI) that Business Associate or its Subcontractors still maintain in any form, and shall retain no copies of such PHI, except as provided herein. Upon Covered Entities' request, Business Associate shall certify in writing that such return or destruction has occurred. If Business Associate determines that return or destruction is not feasible, Business Associate shall explain to Covered Entities in writing why conditions make the return or destruction of such PHI not feasible. If Covered Entities agree that the return or destruction of PHI is not feasible, Business Associate shall retain the PHI, subject to all of the protections of this BAA, and shall make no further Use or Disclosure of the PHI, except as for those purposes that make the return or destruction of the PHI not feasible. In any event, upon termination of the Business Relationship between the parties and/or the BAA, Business Associate shall retain Accounting Information compiled by Business Associate pursuant to Section 2.8 of this BAA for the periods of time required by the Privacy Rule and the HITECH Act, and shall make such Accounting Information available to Covered Entities in accordance with Section 2.8 of this BAA.

4.4. Survival. The obligations of Business Associate under this Section 4 shall survive the termination of the Business Relationship between the parties and/or the BAA.

KAISER PERMANENTE

5 MISCELLANEOUS

5.1 Assistance. In the event of an administrative or judicial action commenced against Covered Entities where Business Associate may be at fault, in whole or in part, as the result of its performance under this BAA, Business Associate agrees to defend or to cooperate with Covered Entities in the defense against such action.

5.2 Subcontracts and Assignment. Business Associate shall not assign its rights or delegate its duties under this BAA without the express written consent of Covered Entities. Subject to the provisions of this BAA, including, without limitation, Section 2.4, Business Associate may subcontract its obligations under this BAA only in connection with a subcontract of its obligations under the parties' Business Relationship, which shall be subject to the terms of such Business Relationship.

5.3 Changes to BAA. Covered Entities reserve the right to change or modify this BAA if required for conformity with federal or state law or if Covered Entities conclude that an amendment to this BAA is reasonably necessary for Covered Entities' operations. Covered Entities will provide notice by posting the updated BAA on Covered Entities' website (http://supplier.kp.org/formsreqs/index.html), with a revised date at the bottom of the BAA. Any changes or modifications will be effective from the day the updated BAA is published. Business Associate acknowledges that its continued Business Relationship with Covered Entities following such notice constitutes its acceptance of the modified BAA.

5.4 Business Relationship. Except as specifically required to implement the purposes of this BAA, and except to the extent inconsistent with this BAA, all terms of the Business Relationship between the parties shall remain in full force and effect. Except as otherwise specifically provided in this BAA or the Business Relationship, in the event of a conflict between the terms of the Business Relationship between the parties and this BAA, this BAA shall control.

5.5 Ambiguity. Any ambiguity in this BAA relating to the Use and Disclosure of PHI shall be resolved in favor of a meaning that furthers the obligations to protect the privacy and security of the PHI, whether electronic or other medium, in accordance with HIPAA and the HIPAA Regulations.

5.6 Compliance with other Laws. In addition to HIPAA and all applicable HIPAA Regulations, Business Associate shall comply with all applicable state and federal security and privacy laws.

5.7 Third Party Beneficiaries. Except as expressly provided for in this BAA or as required by law, there are no third party beneficiaries to this BAA.

5.8 Notices. In addition to the breach notification required in Section 2.13 above, all notices required or permitted to be given under this BAA shall be provided as set forth below:

If to Covered Entities: Sent to the Covered Entities party as set forth in the applicable service agreement. **With a copy via email to:** email: B2PNotices@kp.org **And a copy via written notice and email:** Privacy, Security and Technology Compliance Kaiser Permanente One Kaiser Plaza, 19th Floor Oakland, CA 94612 Attn: Privacy Compliance Email: PrivacyIncidents@kp.org	**If to Business Associate:** Sent to the Business Associate as set forth in the applicable service agreement.