ATTACHMENT B

BUSINESS ASSOCIATE AGREEMENT

Except as otherwise provided in this Agreement, Vanir Construction Management, Inc. hereinafter referred to as BUSINESS ASSOCIATE, may use, access or disclose Protected Health Information to perform functions, activities or services for or on behalf of the COUNTY OF SAN BERNARDINO, hereinafter referred to as the COVERED ENTITY, as specified in this Agreement and the attached **CONTRACT**, provided such use, access or disclosure does not violate the Health Insurance Portability and Accountability Act (HIPAA), 42 United States Code (USC) 1320d et seq., and its implementing regulations, including but not limited to, 45 Code of Federal Regulations (CFR) Parts 160, 162, and 164, hereinafter referred to as the Privacy and Security Rules and patient confidentiality regulations, including but not limited to, California Civil Code 56 – 56.16, 56.20, 56.36, and Health and Safety Codes 1280.1, 1280.3, 1280.15, 130200 and the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009, Public Law 111-5 (the"HITECH Act") and any regulations adopted or to be adopted pursuant to the HITECH Act that relate to the obligations of business associates. Business Associate recognizes and agrees it is obligated by law to meet the applicable provisions of the HITECH Act.

I. Definitions.

a. "Breach" means the acquisition, access, use or disclosure of Protected Health Information (PHI) in a manner not permitted under HIPAA (45 CFR Part 164, Subpart E), CA and/or Civil Code 56.36 which compromises the security or privacy of the Protected Health Information. For the purposes of HITECH, a breach shall not include:

1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of Covered Entity or the Business Associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule; or

2. Any inadvertent disclosure by a person who is authorized to access PHI at Covered Entity or Business Associate to another person authorized to access Protected Health Information at Covered Entity or Business Associate, respectively, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or

3. A disclosure of PHI where Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

b. "Business Associate" means with respect to a Covered Entity, a person who:

1. On behalf of such Covered Entity, but other than in the capacity of a member of the workforce of such Covered Entity performs or assists in the performance of :

(a) a function or activity involving the use or disclosure of Personally Identifiable Health Information, including claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(b) any other function or activity regulated by the HIPAA Privacy or HIPAA Security Regulations; or

2. Provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data Aggregation, management, administrative, accreditation or financial services to or for such Covered Entity where the provision of the service involves the disclosure of Personally Identifiable Health Information from such Covered Entity to the person.

c. "Patient/Client" means Covered Entity funded person who is the patient or client of the Business Associate.

d. "Covered Entity" means a health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA Privacy and Security Regulations.

e. "Data Aggregation" means, with respect to PHI created or received by a Business Associate in its capacity as the Business Associate of a Covered Entity, the combining of such PHI by the Business Associate with the PHI received by the Business Associate in its capacity as a Business Associate of another Covered Entity, to permit data analyses that relate to the health care operations of the respective Covered Entities.

f. "Discovered" means a breach shall be treated as discovered by Covered Entity or Business Associate as the first day on which such breach is known to such Covered Entity or Business Associate, respectively, (including any person, other than the individual committing the breach, that is an employee, officer or other agent of such entity or associate, respectively) or should reasonably have been known to such Covered Entity or Business Associate (or person) to have occurred.

g. "Electronic Protected Health Information" or "Electronic PHI" means PHI that is transmitted by or maintained in electronic media as defined in the HIPAA Security Regulations.

h. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

i. "HIPAA Privacy Rule" means the regulations promulgated under HIPAA by the United States Department of Health and Human Services to protect the privacy of Protected Health Information, including, but not limited to, 45 CFR Part 160 and 45 CFR Part 164, Subpart A and Subpart E.

j. "HIPAA Security Rule" means the regulations promulgated under HIPAA by the United States Department of Health and Human Services to protect the security of Electronic Protected Health Information, including, but not limited to, 45 CFR Part 160 and 45 CFR Part 164, Subpart A and Subpart C.

k. "HITECH Act" means the privacy, security and security Breach notification provisions applicable to Business Associate under Subtitle D of the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which is Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5), and any regulations promulgated thereunder.

l. "Personally Identifiable Health Information" means information that is a subset of health information, including demographic information collected from an individual, and;

1. is created or received by a health care provider, health plan, employer or health care clearinghouse; and

2. 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; and

(a) that identifies the individual; or

(b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

m. "Protected Health Information" or "PHI" means Personally Identifiable Health Information transmitted or maintained in any form or medium that (i) is received by Business Associate from Covered Entity, (ii) Business Associate creates for its own purposes from Personally Identifiable Health Information that Business Associate received from Covered Entity, or (iii) is created, received, transmitted or maintained by Business Associate on behalf of Covered Entity. Protected Health Information excludes Personally Identifiable Health Information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. Section 1232(g), records described at 20 U.S.C. Section 1232g(a)(4)(B)(iv), and employment records held by the Covered Entity in its role as employer.

n. "Secured PHI" means PHI that was rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of technologies or methodologies specified under Section 13402 (h)(2) of the HITECH Act under ARRA.

o. "Unsecured PHI" means PHI that is not secured through the use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services.

p. Any terms capitalized, but not otherwise defined, in this Agreement shall have the same meaning as those terms have under HIPAA, the HIPAA Privacy Rule, the HIPAA Security Rule and the HITECH Act.

II. Obligations and Activities of Business Associate.

a. Permitted Uses. Business Associate shall not use, access or further disclose Protected Health Information other than as permitted or required by this Agreement and as specified in the attached **CONTRACT** or as required by law. Further, Business Associate shall not use Protected Health Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act. Business Associate shall disclose to its employees, subcontractors, agents, or other third parties, and request from Covered Entity, only the minimum Protected Health Information necessary to perform or fulfill a specific function required or permitted hereunder.

b. Prohibited Uses and Disclosures. Business Associate shall not use or disclose Protected Health Information for fundraising or marketing purposes. Business Associate shall not disclose Protected Health 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 Protected Health Information solely relates; 42 U.S.C. Section 17935(a) and 45 C.F.R. section 164.522(a)(1)(i)(A). Business Associate shall not directly or indirectly receive remuneration in exchange for Protected Health Information, except with the prior written consent of Covered Entity and as permitted by the HITECH Act, 42 U.S.C. Section 17935(d)(2); however, this prohibition shall not affect payment by Covered Entity to Business Associate for services provided pursuant to this Agreement.

c. Appropriate Safeguards. Business Associate shall implement the following administrative, physical, and technical safeguards in accordance with the Security Rule under 45 C.F.R., Sections 164.308, 164.310, 164.312 and 164.316:

1. Implement policies and procedures to prevent, detect, contain and correct security violations; identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity; implement a security awareness and training program for all members of its workforce; implement P&Ps to prevent those workforce members who do not have access from obtaining access to electronic PHI; implement policy and procedures to address security incidents; establish policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic PHI; and perform a periodic technical and nontechnical evaluation in response to environmental or operational changes affecting the security of electronic PHI that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

2. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed; implement policies and procedures that specify the proper functions to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic PHI; implement physical safeguards for all workstations that access electronic PHI; restrict access to authorized users; implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility and the movement of these items within the facility.

3. Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights as specified in 45 C.F.R., Section 164.208; implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI; implement policies and procedures to protect electronic PHI from improper alteration, destruction, unauthorized access or loss of integrity or availability.

d. Mitigation. Business Associate shall have procedures in place to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use, access or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

e. Reporting of Improper Access, Use or Disclosure or Breach. Business Associate shall report to Covered Entity's Office of Compliance any unauthorized use, access or disclosure of unsecured Protected Health Information or any other security incident with respect to Protected Health Information no later than two (2) business days upon the discovery of potential breach. Additionally, effective February 17, 2010, the Business Associate shall report to the Covered Entity's Office of Compliance any breach consistent with the regulations promulgated under HITECH by the United States Department of Health and Human Services, 45 CFR Part 164, Subpart D, within two (2) business days of discovery of the potential breach. Upon discovery of the potential breach, the Business Associate shall complete the following actions:

(1) Provide Covered Entity's Office of Compliance with the following information to include but not limited to:

(a) Date the potential breach occurred;
(b) Date the potential breach was discovered;
(c) Number of staff, employees, subcontractors, agents or other third parties and the titles of each person allegedly involved;
(d) Number of potentially affected patients/clients; and
(e) Description of how the potential breach allegedly occurred.

(2) Conduct and document a risk assessment by investigating without reasonable delay and in no case later than twenty (20) calendar days of discovery of the potential breach to determine the following:
(a) Whether there has been an impermissible use, acquisition, access or disclosure of PHI under the Privacy Rule;
(b) Whether an impermissible use or disclosure compromises the security or privacy of the PHI by posing a significant risk of financial, reputational or other harm to the patient/client; and
(c) Whether the incident falls under one of the breach exceptions.

(3) Provide completed risk assessment and investigation documentation to Covered Entity's Office of Compliance within twenty-five (25) calendar days of discovery of the potential breach with decision whether a breach has occurred.:

(a) If a breach has not occurred, notification to patient/client(s) is not required.
(b) If a breach has occurred, notification to the patient/client(s) is required, and Business Associate must provide Covered Entity with affected patient/client names and contact information so the Covered Entity can provide notification.

(4) Make available to Covered Entity and governing State and Federal agencies in a time and manner designated by Covered Entity or governing State and Federal agencies, any policies, procedures, internal practices and records relating to a potential breach for the purposes of audit or should the Covered Entity reserve the right to conduct its own investigation and analysis.

f. Permitted Disclosures. If Business Associate discloses Protected Health Information to a third party, including any agent or subcontractor, Business Associate must obtain, prior to making any such disclosure, (i) reasonable assurances from such third party that such Protected Health Information will be held confidential as provided pursuant to this Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) an agreement from such third party to immediately notify Business Associate of any breach of confidentiality of the Protected Health 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)].

g. Access to Protected Health Information. Business Associate shall provide access to Protected Health Information in a Designated Record Set to Covered Entity or to an Individual, at the request or direction of Covered Entity and in the time and manner designated by the Covered Entity, as required by of 45 CFR 164.524.

h. Amendment of Protected Health Information. If Business Associate maintains a Designated Record Set on behalf of the Covered Entity, Business Associate shall make any amendment(s) to Protected Health Information in a Designated Record Set that the

Covered Entity directs or agrees to, pursuant to 45 CFR 164.526, in the time and manner designated by the Covered Entity.

i. **Access to Records.** Business Associate shall make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use, access and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, and/or to the Secretary for the U.S. Department of Health and Human Services, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy and Security Rules and patient confidentiality regulations.

j. **Audit and Monitor.** Covered Entity reserves the right to audit and monitor all records, policies, procedures and other pertinent items related to the use, access and disclosure of Protected Health Information of the Business Associate as requested to ensure Business Associate is in compliance with this Agreement. Covered Entity has the right to monitor Business Associate in the delivery of services provided under this Agreement. Business Associate shall give full cooperation in any auditing or monitoring conducted.

k. **Accounting for Disclosures.** Business Associate shall document such disclosures of Protected Health Information 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 Protected Health Information. Further, Business Associate shall provide to Covered Entity or an Individual, in the time and manner designated by the Covered Entity, information collected in accordance with provision (i), above, to permit Covered Entity to respond to a request by the Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528 and the HITECH Act.

l. **Destruction of Protected Health Information.** Upon termination of this Agreement, Business Associate shall return all Protected Health Information required to be retained and return or destroy all other Protected Health Information received from the Covered Entity, or created or received by the Business Associate or its subcontractors, employees or agents on behalf of the Covered Entity. In the event the Business Associate determines that returning the Protected Health Information is not feasible, the Business Associate shall provide the Covered Entity with written notification of the conditions that make return not feasible. Business Associate further agrees to extend any and all protections, limitations, and restrictions contained in this Agreement, to any Protected Health Information retained by Business Associate or its subcontractors, employees or agents after the termination of this Agreement, and to limit any further use, access or disclosures to the purposes that make the return or destruction of the Protected Health Information infeasible.

m. **Breach Pattern or Practice by Covered Entity.** Pursuant to 42 U.S.C. Section 17934(b), if the Business Associate knows of a pattern of activity or practice of the Covered Entity that constitutes a material breach or violation of the Covered Entity's obligations under this Agreement, the Business Associate must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, the Business Associate must terminate the Agreement if feasible, or if termination is not feasible, report the problem to the Secretary of DHHS.

n. **Costs Associated to Breach.** Business Associate shall be responsible for reasonable costs associated with a breach. Costs shall be based upon the required notification type as deemed appropriate and necessary by the Covered Entity and shall not be

reimbursable under the contract at any time. Covered Entity shall determine the method to invoice the Business Associate for said costs. Costs shall incur at the current rates and may include, but are not limited to the following:

1. Postage;
2. Alternative means of notice;
3. Media notification; and
4. Credit monitoring services.

III. Specific Use and Disclosure Provisions.

a. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

b. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are required by law.

c. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation service to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).

d. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 42 CFR 164.502(j)(1).

IV. Obligations of Covered Entity.

a. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use, access or disclosure of Protected Health Information.

b. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an individual to use, access or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use, access or disclosure of Protected Health Information.

c. Covered Entity shall notify Business Associate of any restriction to the use, access or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use, access or disclosure of Protected Health Information.

d. Covered Entity shall complete the following in the event that the Covered Entity has determined that Business Associate has a breach:

1. Determine appropriate method of notification to the patient/client(s) regarding a breach as outlined under Section 13402(e) of the HITECH Act;
2. Send notification to the patient/client(s) without unreasonable delay but in no case later than sixty (60) days of discovery of the breach with at least the minimal required elements as follows:
    a. Brief description of what happened, including the date of the breach and the date of discovery;

b. Description of the types of unsecured PHI involved in the breach (such as name, date of birth, home address, Social Security number, medical insurance, etc.);
c. Steps patient/client(s) should take to protect themselves from potential harm resulting from the breach;
d. Brief description of what is being done to investigate the breach, to mitigate harm to patient/client(s) and to protect against any further breaches; and
e. Contact procedures for patient/client(s) to ask questions or learn additional information, which must include a toll-free telephone number, an e-mail address, Web site or postal address.

3. Determine if notice is required to Secretary of the U.S. Department of Health and Human Services.

4. Submit breach information to the Secretary of the U.S. Department of Health and Human Services within the required timeframe, in accordance with 164.408(b).

V. General Provisions.

a. Remedies. Business Associate agrees that Covered Entity shall be entitled to seek immediate injunctive relief as well as to exercise all other rights and remedies which Covered Entity may have at law or in equity in the event of an unauthorized use, access or disclosure of Protected Health Information by Business Associate or any agent or subcontractor of Business Associate that received Protected Health Information from Business Associate.

b. Ownership. The Protected Health Information shall be and remain the property of the Covered Entity. Business Associate agrees that it acquires no title or rights to the Protected Health Information.

c. Regulatory References. A reference in this Agreement to a section in the Privacy and Security Rules and patient confidentiality regulations means the section as in effect or as amended.

d. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy and Security Rules and the Health Insurance Portability and Accountability Act and patient confidentiality regulations.

e. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy and Security Rules and patient confidentiality regulations.

The undersigned affirms that he/she is a duly authorized representative of the Business Associate for which he/she is signing and has the authority to execute this Agreement on behalf of the Business Associate.

Covered Entity	**Business Associate**
COUNTY OF SAN BERNARDINO	
Signature	**Signature**
Dated	**Dated**
Hueston Whiteside	
Name	**Name**
Director, Department of Risk Management	
Title	**Title**