**Business Associate Agreement**

This Business Associate Agreement is entered into by and between Kern Health Systems, a county health authority ("KHS"), and _____, a _____ ("Business Associate"), effective _____ ("Effective Date"). KHS and Business Associate are each a party to this Agreement and are collectively referred to as the "parties." Any extensions or renegotiations of this Agreement shall be reviewed by both parties.

**RECITALS**

WHEREAS, the parties have executed an agreement(s) whereby Business Associate provides services to KHS, and Business Associate creates, receives, maintains, uses, transmits protected health information ("PHI") in order to provide those services ("Professional Services Agreement(s)");

WHEREAS, as a covered entity, KHS is subject to the Administrative Simplification requirements of the Health Insurance Portability and Accountability Act ("HIPAA") of 1996, Public Law 104-191, and regulations promulgated thereunder, including the Standards for Privacy of Individually Identifiable Health Information at 45 Code of Federal Regulations (C.F.R.) Parts 160 and Subparts A and E of 45 C.F.R. Part 164 ("Privacy Regulations") and the Security Standards for Electronic Protected Health Information ("Security Regulations") at 45 C.F.R. Parts 160 and Subparts A and C of 45 C.F.R. Part 164, as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") of 2009, Public Law 111-5, and regulations promulgated thereunder including the Breach Notification Regulations at Subpart D of 45 C.F.R. Part 164, and is subject to certain state privacy laws;

WHEREAS, as a business associate, Business Associate is subject to certain provisions of HIPAA, and regulations promulgated thereunder, as required by the HITECH Act and regulations promulgated thereunder;

WHEREAS KHS and Business Associate are required to enter into a contract in order to mandate certain protections for the privacy and security of PHI;

WHEREAS, KHS'**s** regulator(s) have adopted certain administrative, technical and physical safeguards deemed necessary and appropriate by it/them to safeguard regulators' PHI and have required that KHS incorporate such requirements in its business associate agreements with subcontractors that require access to the regulators' PHI;

NOW, THEREFORE, in consideration of the foregoing, and for other good and valuable consideration, the receipt and adequacy of which is hereby acknowledged, the parties agree as follows:

1. **Definitions**. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in HIPAA, the HITECH Act, and regulations promulgated thereunder.

   1.1. **Agreement** as used in this document means this Business Associate Agreement.

   1.2. **Breach** means, unless expressly excluded under 45 C.F.R. § 164.402, the acquisition, access, use, or disclosure of PHI in a manner not permitted under Subpart E of 45 C.F.R. Part 164 which compromises the security or privacy of the PHI and as more particularly defined under 45 C.F.R. § 164.402.

1.3. **Business Associate** has the meaning given such term in 45 C.F.R. § 160.103.

1.4. **Confidential Information** refers to information not otherwise defined as PHI in Section 1.15 below, but to which state and/or federal privacy and/or security protections apply.

1.5. **Data Aggregation** has the meaning given such term in 45 C.F.R. § 164.501.

1.6. **Designated Record Set** has the meaning given such term in 45 C.F.R. § 164.501.

1.7. **Disclose** and **Disclosure** mean the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

1.8. **Electronic Health Record** has the meaning given such term in 42 U.S.C. § 17921.

1.9. **Electronic Media** means:

1.9.1. Electronic storage material on which data is or may be recorded electronically including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

1.9.2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

1.10. **Electronic Protected Health Information** ("ePHI") means individually identifiable health information that is transmitted by or maintained in electronic media.

1.11. **Health Care Operations** has the meaning given such term in 45 C.F.R. § 164.501.

1.12. **Individual** means the person who is the subject of PHI and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

1.13. **Individually Identifiable Health Information** means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or 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, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 C.F.R. § 160.103.

1.14. **Information System** means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

1.15. **Protected Health Information** ("PHI"), as used in this Agreement and unless otherwise stated, refers to and includes both PHI as defined at 45 C.F.R. § 160.103 and personal information ("PI") as defined in the Information Practices Act at California Civil Code § 1798.3(a). PHI includes information in any form, including paper, oral, and electronic.

1.16. **Required by Law** means a mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing benefits.

1.17. **Secretary** means the Secretary of the U.S. Department of Health and Human Services or the Secretary's designee.

1.18. **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.

1.19. **Services** means those services performed by Business Associate pursuant to the Professional Services Agreement .

1.20. **Unsecured Protected Health Information** ("unsecured PHI") means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under 42 U.S.C. § 17932(h)(2).

1.21. **Use** and **Uses** mean, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination or analysis of such information within the entity that maintains such information.

2. KHS intends that Business Associate may create, receive, maintain, transmit or aggregate certain information pursuant to the terms of this Agreement, some of which information may constitute PHI and/or Confidential Information protected by federal and/or state laws.

3. Business Associate is the business associate of KHS acting on KHS's behalf and provides services or arranges, performs or assists in the performance of functions or activities on behalf of KHS, and may create, receive, maintain, transmit, aggregate, use or disclose PHI (collectively, "use or disclose PHI") in order to fulfill Business Associate's obligations under this Agreement.

4. **Permitted Uses and Disclosures of PHI by Business Associate**. Except as otherwise indicated in this Agreement, Business Associate may use or disclose PHI, inclusive of de-identified data derived from such PHI, only to perform functions, activities or services specified in this Agreement on behalf of KHS, provided that such use or disclosure would not violate HIPAA, including the Privacy Regulations, if done by KHS.

4.1. **Specific Use and Disclosure Provisions**. Except as otherwise indicated in this Agreement, Business Associate may use and disclose PHI if necessary for the proper management and

administration of Business Associate or to carry out the legal responsibilities of Business Associate. Business Associate may disclose PHI for this purpose if the disclosure is required by law, or Business Associate obtains reasonable assurances, in writing, from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.

4.2. **Data Aggregation**. If authorized as part of the services provided to KHS under the Professional Services Agreement, Business Associate may use PHI to provide data aggregation services relating to the health care operations of KHS.

5. **Prohibited Uses and Disclosures of PHI**

5.1. **Restrictions on Certain Disclosures to Health Plans**. Business Associate shall not disclose PHI about an individual to a health plan for payment or health care operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction in accordance with HIPAA and the HITECH Act, including 45 C.F.R. § 164.522(a). The term PHI, as used in this Section, only refers to PHI as defined in 45 C.F.R. § 160.103.

5. 2. **Prohibition on Sale of PHI; No Remuneration**. Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written authorization of KHS and KHS's regulator(s), as applicable, and then, only as permitted by HIPAA and the HITECH Act. The term PHI, as used in this Section, only refers to PHI as defined in 45 C.F.R. § 160.103.

6. **Compliance with Other Applicable Laws**

6.1. To the extent that other state and/or federal laws provide additional, stricter and/or more protective (collectively, "more protective") privacy and/or security protections to PHI or other Confidential Information covered under this Agreement beyond those provided through HIPAA, Business Associate agrees:

6.1.1. To comply with the more protective of the privacy and security standards set forth in applicable state or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the individuals whose information is concerned; and

6.1.2. To treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate, pursuant to Section 17 of this Agreement.

6.2 Examples of laws that provide additional and/or stricter privacy protections to certain types of PHI and/or Confidential Information, as defined in Section 1 of this Agreement, include, but are not limited to the Information Practices Act, California Civil Code §§ 1798-1798.78, Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2, Welfare and Institutions Code § 5328, and California Health and Safety Code § 11845.5.

6.3 If Business Associate is a Qualified Service Organization ("QSO"), as defined in 42 C.F.R.

§ 2.11, Business Associate agrees to be bound by and comply with subdivisions (2)(i) and (2)(ii) under the definition of QSO in 42 C.F.R. § 2.11.

7. **Additional Responsibilities of Business Associate**

7.1. **Nondisclosure**. Business Associate shall not use or disclose PHI or other Confidential Information other than as permitted or required by this Agreement or as required by law.

7.2. **Safeguards and Security**

7.2.1. Business Associate shall use safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI and other confidential data and comply, where applicable, with Subpart C of 45 C.F.R. Part 164 with respect to ePHI, to prevent use or disclosure of the information other than as provided for by this Agreement. Such safeguards shall be, at a minimum, at Federal Information Processing Standards ("FIPS") Publication 199 protection levels. Business Associate shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of Subpart C of 45 C.F.R. Part 164, in compliance with 45 C.F.R. § 164.316. Business Associate shall maintain a comprehensive written information privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of Business Associate's operations and the nature and scope of its activities.

7.2.2. Business Associate shall, at a minimum, utilize an industry-recognized security framework when selecting and implementing its security controls, and shall maintain continuous compliance with its selected framework as it may be updated from time to time. Examples of industry-recognized security frameworks include but are not limited to:

7.2.2.1. NIST SP 800-53 - National Institute of Standards and Technology Special Publication 800-53

7.2.2.2. FedRAMP - Federal Risk and Authorization Management Program

7.2.2.3. PCI - PCI Security Standards Council

7.2.2.4. ISO/ESC 27002 - International Organization for Standardization / International Electrotechnical Commission standard 27002

7.2.2.6. IRS PUB 1075 - Internal Revenue Service Publication 1075

7.2.2.7. HITRUST CSF - HITRUST Common Security Framework

7.2.3. Business Associate shall employ FIPS 140-2 compliant encryption of PHI at rest and in motion unless Business Associate determines it is not reasonable and appropriate to do so based upon a risk assessment, and equivalent alternative measures are in place and documented as such. Business Associate shall maintain, at a minimum, the most current industry standards for

transmission and storage of PHI and other Confidential Information, including, but not limited to, encryption of all workstations, laptops, and removable media devices containing PHI and data transmissions of PHI.

[*Alternate Provision for Section 7.2.3*: "Business Associate shall maintain, at a minimum, the most current industry standards for transmission and storage of PHI and other Confidential Information. Without limiting the foregoing, Business Associate shall maintain, at a minimum, the most current industry standards, for encryption of all workstations, laptops, and removable media devices containing PHI and data transmissions of PHI, unless Business Associate complies with applicable requirements of the Security Regulations, including 45 C.F.R. §§ 164.306 and 164.312."]

7.2.4. Business Associate shall apply security patches and upgrades, and keep virus software up-to-date, on all systems on which PHI and other Confidential Information may be used.

7.2.5. Business Associate shall ensure that all members of its workforce with access to PHI and/or other Confidential Information sign a confidentiality statement prior to access to such data. The statement must be renewed annually.

7.2.6. Business Associate shall identify the security official who is responsible for the development and implementation of the policies and procedures required by 45 C.F.R. Part 164, Subpart C.

7.3. **Minimum Necessary**. With respect to any permitted use, disclosure, or request of PHI under this Agreement, Business Associate shall make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request respectively, as specified in 45 C.F.R. § 164.502(b).

7.4. **Business Associate's Agent**. Business Associate shall ensure that any agents, subcontractors, subawardees, vendors or others (collectively, "agents") that use or disclose PHI and/or Confidential Information on behalf of Business Associate agree through a written agreement to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such PHI and/or Confidential Information.

8. **Mitigation of Harmful Effects**. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI and other Confidential Information in violation of the requirements of this Agreement.

9. **Access to PHI**. Business Associate shall, to the extent KHS determines that any PHI constitutes a designated record set, make the PHI specified by KHS available to the individual(s) identified by KHS as being entitled to access and copy that PHI. Business Associate shall provide such access for inspection of that PHI within fifteen (15) calendar days after receipt of request from KHS. Business Associate shall also provide copies of that PHI ten (10) calendar days after receipt of request from KHS. If Business Associate maintains an electronic health record with PHI, and an individual requests a copy of such information in electronic format, Business Associate shall make such information available in that format as required under the HITECH Act and 45 C.F.R. § 164.524(c)(2)(ii).

10. **Amendment of PHI**. Business Associate shall, to the extent KHS determines that any PHI

constitutes a designated record set, make PHI available for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. § 164.526 as requested by KHS in the time and manner designated by KHS.

11. **Accounting of Disclosures**. Business Associate shall document and make available to KHS or (at the direction of KHS) to an individual, such disclosures of PHI and information related to such disclosures, necessary to respond to a proper request by the subject individual for an accounting of disclosures of PHI in accordance with HIPAA, the HITECH Act and implementing regulations. Unless directed by KHS to make available to an individual, Business Associate shall provide to KHS, within thirty (30) calendar days after receipt of request from KHS, information collected in accordance with this Section to permit KHS to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. The term PHI, as used in this Section, only refers to PHI as defined in 45 C.F.R. § 160.103. Any accounting provided by Business Associate under this Section shall include:

    11.1. The date of the disclosure;

    11.2. The name, and address if known, of the entity or person who received the PHI;

    11.3. A brief description of the PHI disclosed; and

    11.4. A brief statement of the purpose of the disclosure.

    For each disclosure that could require an accounting under this Section, Business Associate shall document the information enumerated above, and shall securely maintain the information for six (6) years from the date of the disclosure (but beginning no earlier than April 14, 2003).

12. **Compliance with HITECH Act**. Business Associate shall comply with the requirements of Title XIII, Subtitle D, of the HITECH Act, which are applicable to business associates, and shall comply with the regulations promulgated thereunder.

13. **Compliance with Obligations of KHS or DHCS**. To the extent Business Associate is to carry out an obligation of KHS or the California Department of Healthcare Services ("DHCS") under 45 C.F.R. Part 164, Subpart E, Business Associate shall comply with the requirements of such Subpart that apply to KHS or DHCS, as applicable, in the performance of such obligation.

14. **Access to Practices, Books and Records**. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI on behalf of KHS available to KHS upon reasonable request, and to the DHCS and the Secretary for purposes of determining KHS's compliance with 45 C.F.R. Part 164, Subpart E. Business Associate also agrees to make its internal practices, books and records relating to the use and disclosure of PHI on behalf of KHS available to DHCS, KHS, and the Secretary for purposes of determining Business Associate's compliance with applicable requirements of HIPAA, the HITECH Act, and implementing regulations. Business Associate shall immediately notify KHS of any requests made by DHCS or the Secretary and provide KHS with copies of any documents produced in response to such request.

15. **Return or Destroy PHI on Termination; Survival**. At termination of this Agreement, if feasible, Business Associate shall return to KHS or, if agreed to by KHS, destroy all PHI and other Confidential Information received from, or created or received by Business Associate on behalf of, KHS that Business Associate or its agents or subcontractors still maintains in any form, and shall retain no copies of such information. If KHS elects destruction of PHI and/or other Confidential

Information, Business Associate shall ensure such information is destroyed in accordance with the destruction methods specified in Sections 15.1 and 15.2 below and shall certify in writing to KHS that such information has been destroyed accordingly. If return or destruction is not feasible, Business Associate shall notify KHS of the conditions that make the return or destruction infeasible. Subject to the approval of KHS's regulator(s) if necessary, if such return or destruction is not feasible, KHS shall determine the terms and conditions under which Business Associate may retain the PHI. Business Associate shall also extend the protections of this Agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

15.1 **Data Destruction**. Data destruction methods for KHS PHI or Confidential Information must conform to U.S. Department of Defense standards for data destruction DoD 5220.22-M (7 Pass) standard or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of KHS and, if necessary, KHS's regulator(s).

15.2 **Destruction of Hard Copy Confidential Data**. KHS PHI or Confidential Information in hard copy form must be disposed of through confidential means, such as crosscut shredding and pulverizing.

15.3 **Survival**. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

16. **Special Provision for SSA Data**. If Business Associate receives data from or on behalf of KHS that was verified by or provided by the Social Security Administration ("SSA Data") and is subject to an agreement between DHCS and the Social Security Administration, Business Associate shall provide, upon request by KHS, a list of all employees and agents and employees who have access to such data, including employees and agents of its agents, to KHS.

17. **Breaches and Security Incidents**. Business Associate shall implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and take the following steps:

17.1. **Notice to KHS**

17.1.1. **Immediate Notice**. Business Associate shall notify KHS immediately upon the discovery of a suspected breach or security incident that involves SSA Data. This notification will be provided by email upon discovery of the breach. If Business Associate is unable to provide notification by email, then Business Associate shall provide notice by telephone to KHS.

17.1.2. **24-Hour Notice**. Business Associate shall notify KHS within 24 hours by email (or by telephone if Business Associate is unable to email KHS) of the discovery of:

17.1.2.1. Unsecured PHI if the PHI is reasonably believed to have been accessed or acquired by an unauthorized person;

17.1.2.2. Any suspected security incident which risks unauthorized access to PHI and/or other Confidential Information;

17.1.2.3. Any intrusion or unauthorized access, use or disclosure of PHI in

violation of this Agreement; or

17.1.2.4. Potential loss of confidential data affecting this Agreement.

17.1.3. Notice shall be provided to the KHS Privacy Officer ("KHS Contact") using the KHS Contact Information at Section 17.7 below. Such notification by Business Associate shall comply with KHS's form and content requirements for reporting privacy incident and shall include all information known at the time the incident is reported.

17.2. **Required Actions**. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI, Business Associate shall take:

17.2.1. Prompt action to mitigate any risks or damages involved with the security incident or breach;

17.2.2. Any action pertaining to such unauthorized disclosure required by applicable federal and state law; and

17.2.3. Any corrective actions required by KHS or KHS's regulator(s).

17.3. **Investigation**. Business Associate shall immediately investigate such security incident or confidential breach. Business Associate shall comply with KHS's additional form and content requirements for reporting such privacy incident.

17.3.1. Incident details including the date of the incident and when it was discovered;

17.3.2. The identification of each individual whose unsecured PHI has been, or is reasonably believed by Business Associate to have been accessed, acquired, used or disclosed during the breach;

17.3.3. The nature of the data elements involved, and the extent of the data involved in the breach;

17.3.4. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data;

17.3.5. A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized;

17.3.6. A description of the probable causes of the improper use or disclosure;

17.3.7. Any other available information that Business Associate is required to include in notification to the individual under 45 C.F.R. § 164.404(c);

17.3.8. Whether the PHI or confidential data that is the subject of the security incident, breach, or unauthorized use or disclosure of PHI or confidential data included unsecured PHI;

17.3.9. Whether a law enforcement official has requested a delay in notification of individuals of the security incident, breach, or unauthorized use or disclosure

of PHI or confidential data because such notification would impede a criminal investigation or damage national security and whether such notice is in writing; and

17.3.10. Whether Section 13402 of the HITECH Act (codified at 42 U.S.C. § 17932), California Civil Code §§ 1798.29 or 1798.82, or any other federal or state laws requiring individual notifications of breaches are triggered.

17.4. **Complete Report**. Business Associate shall provide a complete written report of the investigation ("Final Report") to the KHS Contact within seven (7) working days of the discovery of the security incident or breach. Business Associate shall comply with KHS's additional form and content requirements for reporting of such privacy incident.

17.4.1. The Final Report shall provide a comprehensive discussion of the matters identified in Section 17.3 above and the following:

17.4.1.1. An assessment of all known factors relevant to a determination of whether a breach occurred under HIPAA and other applicable federal and state laws;

17.4.1.2. A full, detailed corrective action plan, including its implementation date and information on mitigation measures taken to halt and/or contain the improper use or disclosure and to reduce the harmful effects of the breach;

17.4.1.3. The potential impacts of the incident, such as potential misuse of data, identity theft, etc.; and

17.4.1.4. A corrective action plan describing how Business Associate will prevent reoccurrence of the incident in the future. Notwithstanding the foregoing, all corrective actions are subject to the approval of KHS and KHS's regulator(s), as applicable.

17.4.2. If KHS or KHS's regulator(s) requests additional information, Business Associate shall make reasonable efforts to provide KHS with such information. A supplemental written report may be used to submit revised or additional information after the Final Report is submitted.

17.4.3. KHS and KHS's regulator(s), as applicable, will review and approve or disapprove Business Associate's determination of whether a breach occurred, whether the security incident or breach is reportable to the appropriate entities, if individual notifications are required, and Business Associate's corrective action plan.

17.4.4. **New Submission Timeframe**. If Business Associate does not complete a Final Report within the seven (7) working day timeframe specified in Section 17.4 above, Business Associate shall request approval from KHS within the seven (7) working day timeframe of a new submission timeframe for the Final Report. Business Associate acknowledges that a new submission timeframe requires the approval of KHS and, if necessary, KHS's regulator(s).

17.5. **Notification of Individuals**. If the cause of a breach is attributable to Business Associate or its agents, then KHS or, as required by KHS, Business Associate shall notify individuals accordingly and shall pay all costs of such notifications. The notifications shall comply with applicable federal and state law. All such notifications shall be coordinated with KHS. KHS and KHS regulator(s), as applicable, shall approve the time, manner and content of any such notifications. Business Associate acknowledges that such review and approval by KHS and KHS regulator(s), as applicable, must be obtained before the notifications are made.

17.6. **Responsibility for Reporting of Breaches to Entities Other than KHS**. If the cause of a breach of PHI is attributable to Business Associate or its subcontractors, Business Associate agrees that KHS shall make all required reporting of the breach as required by applicable federal and state law, including any required notifications to media outlets, the Secretary, and other government agency/regulator.

17.7. **KHS Contact Information**. To direct communications to KHS Privacy Officer, Business Associate shall initiate contact as indicated here. KHS reserves the right to make changes to the contact information below by giving written notice to Business Associate. These changes shall not require an amendment to this Agreement.

KHS Privacy Officer

c/o: Deborah Murr, Chief Compliance and Fraud Prevention Officer
KHS
2900 Buck Owens Blvd.
Bakersfield, CA 93308

Email: deborah.murr@khs-net.com

Telephone: 661-664-5000

18. **Responsibilities of KHS**

18.1 KHS agrees to not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA and/or other applicable federal and/or state law.

18.2 **Notification of SSA Data**. KHS shall notify Business Associate if Business Associate receives data that is SSA Data from or on behalf of KHS.

19. **Indemnification**. Business Associate will immediately indemnify and pay KHS for and hold it harmless from (i) any and all fees and expenses KHS incurs in investigating, responding to, and/or mitigating a breach of PHI or Confidential Information caused by Business Associate or its subcontractors or agents; (ii) any damages, attorneys' fees, costs, liabilities or other sums actually incurred by KHS due to a claim, lawsuit, or demand by a third party arising out of a breach of PHI or Confidential Information caused by Business Associate or its subcontractors or agents; and/or (iii) for fines, assessments, sanctions, and/or civil penalties assessed or imposed against KHS by any government agency/regulator based on a breach of PHI or Confidential Information caused by Business Associate or its subcontractors or agents. Such fees and expenses may include, without limitation, attorneys' fees and costs and costs for computer security consultants, credit reporting

agency services, postal or other delivery charges, notifications of breach to individuals, and required reporting of breach. Acceptance by KHS of any insurance certificates and endorsements required under the Professional Service Agreement(s) does not relieve Business Associate from liability under this indemnification provision. This provision shall apply to any damages or claims for damages whether or not such insurance policies shall have been determined to apply.

19.1 With respect to any action or claim subject to indemnification herein by Business Associate, Business Associate shall, at its sole cost, have the right to use counsel of its choice, subject to the approval of KHS, which shall not be unreasonably withheld, and shall have the right to adjust, settle, or compromise any such action or claim only with the prior consent of KHS, which shall not be unreasonably withheld; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes Business Associate's indemnification to KHS as set forth herein. Business Associate's obligation to defend, indemnify and hold harmless KHS shall be subject to KHS having given Business Associate written notice within a reasonable period of time of the claim or of the commencement of the related action, as the case may be, and information and reasonable assistance, at Business Associate's expense, for the defense or settlement thereof. Business Associate's obligation hereunder shall be satisfied (if KHS has no liability whatsoever for the claim) when Business Associate has provided to KHS the appropriate form of dismissal relieving KHS from any liability for the action or claim involved.

19.2 In the event there is a conflict between this indemnification clause and the indemnification clause contained in the Professional Services Agreement, this indemnification clause shall only apply to the subject issues set forth in this Business Associate Agreement.

20. **Audits, Inspection and Enforcement**

20.1. From time to time, KHS or KHS's regulator(s) may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Agreement. Business Associate shall promptly remedy any violation of this Agreement and shall certify the same to the KHS Privacy Officer in writing. Whether or how KHS or KHS's regulator(s) exercises this provision shall not in any respect relieve Business Associate of its responsibility to comply with this Agreement.

20.2. If Business Associate is the subject of an audit, compliance review, investigation or any proceeding that is related to the performance of its obligations pursuant to this Agreement, or is the subject of any judicial or administrative proceeding alleging a violation of HIPAA, Business Associate shall promptly notify KHS unless it is legally prohibited from doing so.

21. **Term and Termination**

21.1. **Term.** The term of this Agreement shall be effective as of the Effective Date and shall terminate in either (i) accordance with this Section 21 of this Business Associate Agreement or (ii) when all of the PHI provided by KHS to Business Associate, or created or received by Business Associate on behalf of KHS, is destroyed or returned to KHS in accordance with Section 15 of this Business Associate Agreement. KHS may terminate this BAA, without cause, on five (5) days' prior written notice to Business Associate.

21.2. **Termination for Cause**. Upon KHS's knowledge of a violation of this Agreement by

Business Associate, KHS may in its discretion:

21.2.1. Provide an opportunity for Business Associate to cure the violation and terminate this Agreement if Business Associate does not do so within the time specified by KHS; or

21.2.2. Terminate this Agreement if Business Associate has violated a material term of this Agreement.

21.3. **Judicial or Administrative Proceedings**. KHS may terminate this Agreement if Business Associate is found to have violated HIPAA, or stipulates or consents to any such conclusion, in any judicial or administrative proceeding.

22. **Miscellaneous Provisions**

22.1. **Disclaimer**. KHS makes no warranty or representation that compliance by Business Associate with this Agreement will satisfy Business Associate's business needs or compliance obligations. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI and other Confidential Information.

22.2. **Amendment**

22.2.1. Any provision of this Agreement which is in conflict with current or future applicable federal or state laws is hereby amended to conform to the provisions of those laws. Such amendment of this Agreement shall be effective on the effective date of the laws necessitating it and shall be binding on the parties even though such amendment may not have been reduced to writing and formally agreed upon and executed by the parties.

22.2.2. Failure by Business Associate to take necessary actions required by amendments to this Agreement under Section 22.2.1 of this Agreement shall constitute a material violation of this Agreement.

22.3. **Assistance in Litigation or Administrative Proceedings**. Business Associate shall make itself and its employees and agents available to KHS or KHS's regulator(s) at no cost to KHS or KHS's regulator(s), as applicable, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against KHS or KHS's regulator(s), their respective directors, officers and/or employees based upon claimed violation of HIPAA, which involve inactions or actions by Business Associate.

22.4. **No Third-Party Beneficiaries**. Nothing in this Agreement is intended to or shall confer, upon any third person any rights or remedies whatsoever.

22.5. **Interpretation**. The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA and other applicable laws.

22.6. **No Waiver of Obligations**. No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

22.7. **Statutory or Regulatory Reference**. Any reference to statutory or regulatory language in this Agreement shall be to such language as in effect or as amended.

22.8. **Injunctive Relief**. Notwithstanding any rights or remedies provided in this Agreement, KHS retains all rights to seek injunctive relief to prevent or stop the unauthorized use or disclosure of PHI or Confidential Information by Business Associate or any agent, subcontractor, employee or third party that received PHI or Confidential Information.

22.9 **Monitoring.** As applicable, Business Associate shall comply with monitoring requirements of KHS's contracts with regulator(s) or any other monitoring requests by KHS's regulator(s).

22.10 **Venue**. It is expressly acknowledged that this Agreement has been entered into and will be performed within the County of Kern. Should any suit or action be commenced to enforce or interpret the terms of this Agreement or any claim arising under it, it is expressly agreed that proper venue shall be in County of Kern, State of California.

## EXECUTION

Subject to the execution of a Professional Services Agreement or amendments thereto by Business Associate and KHS, this Business Associate Agreement shall become effective on the Effective Date.

In witness thereof, the parties have executed this Business Associate Agreement:

| Business Associate | KHS |
|---|---|
| _____ | _____ |
| Print Name | Print Name |
| _____ | _____ |
| Signature | Signature |
| _____ | _____ |
| Title | Title |
| _____ | _____ |
| Date | Date |