

**BUSINESS ASSOCIATE AGREEMENT
BETWEEN
CENCAL HEALTH
AND
< _____ >**

This Business Associate Agreement (“BAA”) is entered into by and between Santa Barbara San Luis Obispo Regional Health Authority, dba CenCal Health (“Covered Entity”) and _____ (together with its affiliates “Business Associate”) effective as of January 1, 2024. Business Associate and Covered Entity may be referred to herein individually as a “Party” or collectively as the “Parties.” This BAA supersedes all previously executed Business Associate Agreements executed between the parties as of January 1, 2024.

Covered Entity and Business Associate have entered into, or are contemplating entering into substantially concurrent with this BAA, an agreement pursuant to which Business Associate will provide certain services to Covered Entity (the “Agreement”), which services may involve the disclosure to Business Associate by Covered Entity of Protected Health Information, as defined below. In connection with the performance of services under the Agreement, the parties wish to enter into this BAA to protect the confidentiality and security of any Protected Health Information and to ensure compliance with laws and regulations applicable to such protections.

1. DEFINITIONS

1.1 “HIPAA” shall mean the Health Insurance Portability and Accountability Act of 1996, including its implementing regulations, as such may be amended from time to time.

1.2 “HITECH” shall mean Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009, including its implementing regulations, as such may be amended from time to time.

1.3 “Breach” shall mean the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI as defined, and subject to the exceptions set forth, in 45 C.F.R. 164.402, a State Breach as defined below, or a breach of information subject to 42 C.F.R. Part 2 (“Part 2”).

1.4 “Electronic Protected Health Information” (“ePHI”) shall mean PHI as defined in Section 1.5 that is transmitted or maintained in electronic media.

1.5 “PHI” shall mean Protected Health Information, as defined in 45 C.F.R. § 160.103, and is limited to the Protected Health Information received from, or received or created on behalf of, Covered Entity by Business Associate pursuant to performance of the Services.

1.6 “Privacy Rule” shall mean the federal privacy regulations issued pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended from time to time, codified at 45 C.F.R. Parts 160 and 164 (Subparts A & E).

1.7 “Security Rule” shall mean the federal security regulations issued pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended from time to time, codified at 45 C.F.R. Parts 160 and 164 (Subparts A & C).

1.8 “Security Incident” shall have the meaning, as defined in 45 C.F.R. §164.304, of the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system,

1.9 "Services" shall mean, to the extent and only to the extent they involve the creation, use or disclosure of PHI, the services provided or by Business Associate to Covered Entity under the Agreement, or as described in any other writing executed by the parties and created in anticipation of the Agreement, including those Services set forth in this BAA that involve the use or disclosure of PHI, as any such documents may be amended by written agreement of the Parties from time to time.

1.10 "State Breach" shall mean any unauthorized disclosure of information subject to state breach reporting laws, including but not limited to Information Practices Act, California Civil Code sections 1798.29.

1.11 Unless otherwise specified in this BAA, all capitalized terms used in this BAA, not otherwise defined in this BAA or otherwise in the Agreement, shall have the meanings established for purposes of HIPAA and/or HITECH, as each may be amended from time to time. Capitalized terms used in this BAA that are not otherwise defined in this BAA and that are defined in the Agreement shall have the respective meanings assigned to them in the Agreement. Any and all references in this BAA to sections of HIPAA or HITECH, or the implementing regulations of either, shall be deemed to include all associated existing and future implementing regulations as such may be amended, in all cases when and as each is effective.

2. RESPONSIBILITIES OF BUSINESS ASSOCIATE

With regard to its use and/or disclosure of PHI, Business Associate agrees to:

2.1 use and/or disclose PHI only as necessary to provide the Services, as permitted or required by this BAA, and in compliance with each applicable requirement of 45 C.F.R. § 164.504(e) or as otherwise required by law;

2.2 implement and use appropriate administrative, physical and technical safeguards to (i) prevent use or disclosure of PHI other than as permitted or required by this BAA; (ii) reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that Business Associate creates, receives, maintains, or transmits on behalf of the Covered Entity; and (iii) comply with the Security Rule requirements set forth in 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.316 and applicable Federal Information Processing Standards (FIPS) Publication 199 protection levels;

2.3 as required by the State of California, notify Covered Entity (a) immediately by telephone plus e-mail to Covered Entity's Compliance and Privacy Officer at (805) 685-9525 and HIPAATeam@Cencalhealth.org, of any suspected breach or security incident involving PHI and/or other confidential information, including, but not limited to those involving SSA data, reasonably believed to have resulted in the unauthorized intrusion, access, acquisition, use, disclosure, or potential loss of such PHI or other confidential information, in violation of this BAA, and (b) within twenty-four (24) hours by e-mail or fax of any other suspected Breach or Security Incident of which it becomes aware;

2.4 with respect to any use or disclosure of Unsecured PHI not permitted by the Privacy Rule, or any other Breach or Security Incident, Business Associate shall, without unreasonable delay, and in any event within twenty-four (24) hours after Discovery, provide Covered Entity with written notification thereof and information regarding the data elements involved, extent of the data involved, and identification of unauthorized persons reasonably believed to have improperly used or disclosed confidential data. Covered Entity has the responsibility for determining whether any such incident is a reportable breach under HIPAA. In the event of a Breach, Business Associate's notification should include a list of Individuals impacted. Notice shall be made using the current DHCS "Privacy Incident Reporting Form" ("PIR Form"); and shall include all information known at the time the incident is reported. The form is available online at the DHCS website. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or Personal Information as defined in HIPAA, Business Associate shall take: a. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and b. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations. Business Associate will reimburse Covered Entity for all reasonable out-of-pocket expenses incurred by Covered

Entity in providing all legally required notifications to individuals, the U.S. Department of Health and Human Services ('HHS'), other governmental agencies, and/or the media;

2.5 require all of its subcontractors and agents that create, receive, maintain, or transmit PHI to agree, in writing, to substantially the same restrictions and conditions on the use and/or disclosure of PHI that apply to Business Associate; including but not limited to the extent that Business Associate provides PHI to a subcontractor or agent, it shall require the subcontractor or agent to implement reasonable and appropriate safeguards to protect the PHI and to timely notify the Business Associate of any Breach consistent with the requirements of this BAA;

2.6 make available its internal practices, books, and records relating to the use and disclosure of PHI to the Secretary, when so requested, for purposes of determining Covered Entity's compliance with the Privacy Rule;

2.7 document, and within thirty (30) days after receiving a written request from Covered Entity, make available to Covered Entity such information as is in Business Associate's possession and is required for Covered Entity to make an accounting, in accordance with 45 C.F.R. § 164.528;

2.8 notwithstanding Section 2.7, in the event that Business Associate in connection with the Services uses or maintains an Electronic Health Record of PHI of or about an Individual, then Business Associate shall when and as directed by Covered Entity, make an accounting of disclosures of PHI made by Business Associate to the Covered Entity within thirty (30) days, in accordance with the requirements for accounting for disclosures made through an Electronic Health Record in 42 U.S.C. 17935(c);

2.9 provide access, within thirty (30) days after receiving a written request from Covered Entity to PHI in a Designated Record Set (as defined at 45 C.F.R. § 164.501) about an Individual, directly to Covered Entity in accordance with the requirements of 45 C.F.R. § 164.524;

2.10 notwithstanding Section 2.9, in the event that Business Associate in connection with the Services uses or maintains an Electronic Health Record of PHI of or about an Individual, then Business Associate shall provide an electronic copy of the PHI within thirty (30) days, to Covered Entity, all in accordance with 42 U.S.C. § 17935(e);

2.11 to the extent that the PHI in Business Associate's possession constitutes a Designated Record Set, make available, within thirty (30) days after a written request by Covered Entity, PHI for amendment as directed by Covered Entity, all in accordance with 45 C.F.R. § 164.526;

2.12 request, use and/or disclose only the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure; provided, that Business Associate shall comply with 42 U.S.C. § 17935(b);

2.13 not directly or indirectly receive remuneration in exchange for any PHI as prohibited by 42 U.S.C. § 17935(d);

2.14 not make or cause to be made any communication about a product or service that is prohibited by 42 U.S.C. § 17936(a);

2.15 not make or cause to be made any written fundraising communication that is prohibited by 42 U.S.C. § 17936(b); and

2.16 accommodate reasonable requests by Individuals for confidential communications in accordance with 45 C.F.R. § 164.522(b).

2.17 comply with other applicable State and/or federal privacy and security laws to the extent that such laws provide additional, more stringent, and/or more protective (collectively, "More Protective") privacy

and/or security protections to PHI or personally identifiable information covered under this Agreement beyond those provided through HIPAA, Business Associate agrees:

- a. To comply with the More Protective of the privacy and security standards set forth in applicable State or federal laws, including but not limited to: the Information Practices Act, California Civil Code sections 1798-1798.78, Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2, Welfare and Institutions Code section 5328, and California Health and Safety Code sections 11812, 11845.5, 120975 *et. seq.* 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
 - b. With respect to Part 2 Records (as defined in 42 C.F.R. § 2.11) received from Covered Entity, Business Associate agrees to be bound by the provisions of Part 2 upon receipt of the Records. Business Associate shall not re-disclose patient identifying information to a third party unless that third party is a subcontractor or agent of Business Associate to assist them in providing the Services and only as long as the subcontractor or agent only further discloses the information back to Business Associate or Law.
 - c. To treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate, consistent with this BAA.
- 2.18 to the extent Business Associate is to carry out an obligation of Covered Entity acting on behalf of DHCS under 45 CFR Part 164, Subpart E, comply with the requirements of the subpart that apply to Covered Entity acting on behalf of DHCS in the performance of such obligation.
 - 2.19 if Business Associate receives data from Covered Entity acting on behalf of DHCS that was verified by or provided by the Social Security Administration (SSA data) and is subject to an agreement between DHCS and SSA, Business Associate shall provide, upon request by Covered Entity acting on behalf of DHCS, a list of all employees and agents and employees who have access to such data, including employees and agents of its agents, to Covered Entity acting on behalf of DHCS.
 - 2.20 provide a complete report of the investigation to the Covered Entity acting on behalf of DHCS contacts within ten (10) working days of the discovery of the security incident or breach. The report must include any applicable additional information not included in the Initial Form. The Final report shall include an assessment of all known factors relevant to a determination of whether a breach occurred under HIPAA and other applicable federal and state laws. The report shall also include 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. If Business Associate does not complete a Final report within the ten (10) working day timeframe, Business Associate shall request approval from Covered Entity acting on behalf of DHCS within the ten (10) working day timeframe of a new submission timeframe for the Final report.
 - 2.21 if the cause of a breach is attributable to Business Associate or its agents, Business Associate shall notify individuals accordingly and shall pay all costs of such notifications, as well as all costs associated with the breach. The notifications shall comply with applicable federal and state law.

Covered Entity and DHCS shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.

- 2.22 if the cause of a breach of PHI is attributable to Business Associate or its subcontractors, Business Associate is responsible for all required reporting of the breach as required by applicable federal and state law.
- 2.23 Covered Entity and DHCS may inspect the facilities, systems, books and records of Business Associate to monitor compliance with Covered Entity's contract. 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 Covered Entity acting on behalf of DHCS unless it is legally prohibited from doing so.
- 2.24 be solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI and other confidential information.
- 2.25 Business Associate shall make itself and its employees and agents available to Covered entity and DHCS at no cost to Covered Entity and DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers and/or employees based upon claimed violation of HIPAA, which involve inactions or actions by the Business Associate.

3. RESPONSIBILITIES OF COVERED ENTITY

In addition to any other obligations set forth in the Agreement, including in this BAA, Covered Entity:

- 3.1 shall provide to Business Associate only the minimum PHI necessary to accomplish the Services;
- 3.2 in the event that the Covered Entity honors a request to restrict the use or disclosure of PHI pursuant to 45 C.F.R. § 164.522(a) or makes revisions to its notice of privacy practices of Covered Entity in accordance with 45 C.F.R. § 164.520 that increase the limitations on uses or disclosures of PHI or agrees to a request by an Individual for confidential communications under 45 C.F.R. § 164.522(b), Covered Entity agrees not to provide Business Associate any PHI that is subject to any of those restrictions or limitations to the extent any may limit Business Associate's ability to use and/or disclose PHI as permitted or required under this BAA unless Covered Entity notifies Business Associate of the restriction or limitation and Business Associate agrees to honor the restriction or limitation;
- 3.3 shall be responsible for using administrative, physical and technical safeguards at all times to maintain and ensure the confidentiality, privacy and security of PHI transmitted to Business Associate pursuant to the Agreement, including this BAA, in accordance with the standards and requirements of HIPAA, until such PHI is received by Business Associate; and
- 3.4 shall obtain any consent or authorization that may be required by applicable federal or state laws and regulations prior to furnishing Business Associate the PHI.

4. PERMITTED USES AND DISCLOSURES OF PHI

Unless otherwise limited in this BAA, in addition to any other uses and/or disclosures permitted or required by this BAA, Business Associate may:

- 4.1 make any and all uses and disclosures of PHI necessary to provide the Services to Covered Entity;

4.2 use and disclose to subcontractors and agents the PHI in its possession for its proper management and administration or to carry out the legal responsibilities of Business Associate, provided that any third party to which Business Associates discloses PHI for those purposes provides written assurances in advance that: (i) the information will be held confidentially and used or further disclosed only as Required by Law; (ii) the information will be used only for the purpose for which it was disclosed to the third party; and (iii) the third party promptly will notify Business Associate of any instances of which it becomes aware in which the confidentiality of the information has been breached, in each case in accordance with Section 2.5 of this BAA;

4.3 provide Data Aggregation services relating to the Health Care Operations of Covered Entity in accordance with the Privacy Rule; and

4.4 use the PHI to create a Limited Data Set in compliance with 45 C.F.R. 164.514(e).

5. ADDITIONAL REQUIREMENTS OF COVERED ENTITY AND BUSINESS ASSOCIATE AS REQUIRED BY THE STATE OF CALIFORNIA, DEPARTMENT OF HEALTH CARE SERVICES (“DHCS”)

Covered Entity and/or Business Associate, as applicable, shall:

5.1 comply with all monitoring provisions of Covered Entity’s contract with DHCS and any monitoring requests by the DHCS.

5.2 provide DHCS’ Contracting Officer with a list of external entities, including persons, organizations, and agencies, other than those within its treatment network and other than DHCS, to which it discloses lists of Medi-Cal Member names and addresses? This list must be provided within 30 calendar days of the execution of the state contract and annually thereafter.

5.3 not to divulge the Medi-Cal status of the Covered Entity’s members without DHCS’ prior approval except for treatment, payment and operations, or as required by law.

5.4 to take any and all appropriate steps necessary to ensure the continuous security of all computerized data systems containing PHI, and provide data security procedures for the use of DHCS at the end of the contract period. The steps shall include, at a minimum:

a. comply with all of the data system security safeguards listed in the state contract;

b. achieve and maintain compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164). 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 necessary in conducting operations on behalf of DHCS under the state contract;

c. General Security Controls

- a) Confidentiality Statement. All persons that will be working with DHCS PHI must sign a confidentiality statement supplied by the Covered Entity. The statement must include at a minimum, General Use, Security and Privacy safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DHCS PHI. The statement must be renewed annually.
- b) Background check. Before a member of the Covered Entity’s workforce may access DHCS PHI, Covered Entity must conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk for theft of confidential data.
- c) Workstation/Laptop encryption. All workstations and laptops that process and/or store DHCS PHI must be encrypted with a DHCS approved solution or a solution using a vendor product specified on

the California Strategic Sourced Initiative (CSSI) located at the following link:

www.pd.dgs.ca.gov/masters/EncryptionSoftware.html. The encryption solution must be full disc unless approved by the DHCS Information Security Office.

- d) Only the minimum necessary amount of DHCS PHI may be downloaded to a laptop or hard drive when absolutely necessary for business purposes.
- e) Removable media devices. All electronic files that contain DHCS PHI must be encrypted when stored on any removable media type device (i.e. USB thumb drives, floppies, CD/DVD, etc.) with a DHCS approved solution or a solution using a vendor product specified on the CSSI.
- f) Email security. All emails that include DHCS PHI must be sent in an encrypted method using a DHCS approved solution or a solution using a vendor product specified on the CSSI.
- g) Antivirus software. All workstations, laptops and other systems that process and/or store DHCS PHI must have a commercial third-party anti-virus software solution with a minimum daily automatic update.
- h) Patch Management. All workstations, laptops and other systems that process and/or store DHCS data must have security patches applied and up-to-date.
- i) User IDs and Password Controls. All users must be issued a unique user name for accessing DHCS PHI. Passwords are not to be shared. Must be at least eight characters. Must be a non-dictionary word. Must not be stored in readable format on the computer. Must be changed every 60 days. Must be changed if revealed or compromised. Must be composed of characters from at least three of the following four groups from the standard keyboard:
 - i. Upper case letters (A-Z)
 - ii. Lower case letters (a-z)
 - iii. Arabic numerals (0-9)
 - iv. Non-alphanumeric characters (punctuation symbols)
- j) Data Destruction. All DHCS data must be destroyed using Department of Defense standard methods for data destruction when the DHCS data is no longer needed.
- k) Remote Access. Any remote access to DHCS PHI must be executed over an encrypted method approved by DHCS or using a vendor product specified on the CSSI. All remote access must be limited to minimum necessary and least privilege principles.

d. System Security Controls

- a) System Timeout. The system must provide an automatic timeout after no more than 20 minutes of inactivity.
- b) Warning Banners. All systems containing DHCS PHI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.
- c) System Logging. The system must log success and failures of user authentication at all layers. The system must log all system administrator/developer access and changes if the system is processing and/or storing PHI. The system must log all user transactions at the database layer if processing and/or storing DHCS PHI.
- d) Access Controls. The system must use role based access controls for all user authentication, enforcing the principle of least privilege.
- e) Transmission Encryption. All data transmissions must be encrypted end-to-end using a DHCS approved solution or a solution using a vendor product specified on the CSSI, when transmitting DHCS PHI.
- f) Host Based Intrusion Detection. All systems that are accessible via the Internet or store DHCS PHI must actively use a comprehensive third-party real-time host based intrusion detection and prevention program.

e. Audit Controls

- a) System Security Review. All systems processing and/or storing DHCS PHI must have at least an annual system security review. Reviews must include administrative and technical vulnerability scanning tools.
- b) Log Reviews. All systems processing and/or storing DHCS PHI must have a routine procedure in place to review system logs for unauthorized access. Logs must be maintained for six years after the occurrence.
- c) Change Control. All systems processing and/or storing DHCS PHI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

f. Business Continuity/disaster Recovery Controls

- a) Emergency Mode Operation Plan. Covered Entity must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DHCS PHI in the event of an emergency.
- b) Data Backup Plan. Covered Entity must have established documented procedures to backup DHCS data to maintain retrievable exact copies of DHCS PHI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup tapes, and the amount of time to restore DHCS data should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

g. Paper Document Controls

- a) Supervision of Data. Covered Entity must have a policy that:
 - i. DHCS PHI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information.
 - ii. DHCS PHI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
- b) Escorting Visitors. Visitors to areas where DHCS PHI is contained shall be escorted and DHCS PHI shall be kept out of sight while visitors are in the area unless they are authorized to view the PHI.
- c) Confidential Destruction. DHCS PHI must be disposed of through confidential means, such as shredding and pulverizing.
- d) Removal of Data. DHCS PHI must not be removed from the premises of the Covered Entity except for routine business purposes or with the express written permission of DHCS.
- e) Faxing. Faxes containing DHCS PHI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending.
- f) Mailing. DHCS PHI shall only be mailed using secure methods. Large volume mailings of DHCS PHI shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted.

5.5 To ensure that any agents, including subcontractors but excluding providers of treatment services, to whom Covered Entity provides PHI received from or created or received by Covered Entity on behalf of DHCS, agree to the same restrictions and conditions that apply to Covered Entity with respect to such PHI; and to incorporate, when applicable, the relevant provisions of the state contract into each Subcontract or subaward to such agents or subcontractors.

5.6 To produce a Notice of Privacy Practices (NPP) in accordance with standards and requirements of HIPAA, the HIPAA regulations, applicable State and Federal laws and regulations, and Section 2.A. of this Exhibit. Such NPP's must include the DHCS Privacy Officer contact information included in part H. above of the state contract as an alternative means for Medi-Cal beneficiaries to lodge privacy complaints. All NPP's created or modified after August 1, 2003, must be submitted to Covered Entity's DHCS contract manager for review.

5.7 address the Assistance in Litigation or Administrative Proceedings requirement that the Covered Entity shall make itself and its employees, and use all due diligence to make any subcontractors or agents assisting Covered Entity in the performance of its obligations under the state contract, available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, except where Covered Entity or its subcontractor, employee or agent is a named adverse party.

5.8 To 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. In addition, Business Associate shall maintain, at a minimum, the most current industry standards for transmission and storage of PHI and other confidential information.

5.9 To 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.

5.10 To 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.

5.11 To identify the security official who is responsible for the development and implementation of the policies and procedures required by 45 CFR Part 164, Subpart C.

5.12 To 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 BAA.

5.13 To make its internal practices, books, and records relating to the use and disclosure of PHI on behalf of Covered Entity available to Covered Entity and DHCS upon reasonable request, and to the federal Secretary of Health and Human Services for purposes of determining Covered Entity's compliance with 45 CFR Part 164, Subpart E.

6. INDEMNIFICATION

Business Associate shall indemnify, defend and hold harmless Covered Entity from and against any claims, actions, liabilities, losses or damages, including expenses such as reasonable attorneys' fees and other costs of litigation or dispute resolution in connection with any Breach, as defined above, caused by Business Associate's failure to carry out its responsibilities under Section 2 and Section 5 of this BAA, except to the extent that any such Breach may have been caused by the failure of Covered Entity to meet its obligations under this BAA, the Agreement or under the provisions of HIPAA and HITECH.

7. TERMINATION AND COOPERATION

7.1 Termination. If either Party knows of a pattern of activity or practice of the other Party that constitutes a material breach or violation of this BAA then the non-breaching Party shall provide written notice of the breach or violation to the other Party that specifies the nature of the breach or violation. The breaching Party must cure the breach or end the violation on or before thirty (30) days after receipt of the written notice. In the absence of a cure reasonably satisfactory to the non-breaching Party within the specified timeframe, or in the event the breach is reasonably incapable of cure, then the non-breaching Party may do the following:

- (i) if feasible, terminate the Agreement, including this BAA; or
- (ii) if termination of the Agreement is infeasible, report the issue to HHS.

7.2 Effect of Termination or Expiration. Within sixty (60) days after the expiration or termination for any reason of the Agreement and/or this BAA, Business Associate shall return or destroy all PHI, if feasible to do so, including all PHI in possession of Business Associate's agents or subcontractors. In the event that Business Associate determines that return or destruction of the PHI is not feasible, Business Associate shall notify Covered Entity in writing and may retain the PHI subject to this Section 6.2. Under any circumstances, Business Associate shall extend any and all protections, limitations and restrictions contained in this BAA to Business Associate's use and/or disclosure of any PHI retained after the expiration or termination of the Agreement and/or this BAA, and shall limit any further uses and/or disclosures solely to the purposes that make return or destruction of the PHI infeasible.

7.3 Cooperation. Each Party shall cooperate in good faith in all respects with the other Party in connection with any request by a federal or state governmental authority for additional information and documents or any governmental investigation, complaint, action or other inquiry.

7.4 Return or Destroy PHI on Termination. At termination of this BAA, if feasible, Business Associate shall return or destroy all PHI and other confidential information received from, or created or received by Business Associate on behalf of, Covered Entity that Business Associate still maintains in any form and retain no copies of such information. If return or destruction is not feasible, Business Associate shall notify Covered Entity of the conditions that make the return or destruction infeasible, and Covered Entity and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. If such return or destruction is not feasible, Business Associate shall extend the protections of this BAA to the information and limited further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

8. MISCELLANEOUS

8.1 Contradictory Terms; Construction of Terms. Any other provision of the Agreement that is directly contradictory to one or more terms of this BAA ("Contradictory Term") shall be superseded by the terms of this BAA to the extent and only to the extent of the contradiction, only for the purpose of Covered Entity's and Business Associate's compliance with HIPAA and HITECH, and only to the extent that it is reasonably impossible to comply with both the Contradictory Term and the terms of this BAA. The terms of this BAA to the extent they are unclear shall be construed to allow for compliance by Covered Entity and Business Associate with HIPAA and HITECH.

8.2 Survival. Sections 2.2, 2.3, 2.4, 2.6, 2.7 and 7.2 shall survive the expiration or termination for any reason of the Agreement and/or of this BAA.

8.3 No Third Party Beneficiaries. Nothing in this BAA shall confer upon any person other than the Parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

8.4 Any provision of this BAA 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 BAA 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.

8.5 Independent Contractor. Business Associate and Covered Entity are and shall remain independent contractors throughout the term. Nothing in this BAA or otherwise in the Agreement shall be construed to constitute Business Associate and Covered Entity as partners, joint venturers, agents or anything other than independent contractors.

8.6 Counterparts; Facsimile Signatures. This BAA may be executed in any number of counterparts, each of which will be deemed an original and all of which together will constitute one and the same document. This BAA may be executed and delivered by facsimile or in PDF format via email, and any

such signatures will have the same legal effect as manual signatures. If a Party delivers its executed copy of this BAA by facsimile signature or email, such Party will promptly execute and deliver to the other Party a manually signed original if requested by the other Party.

CENCAL HEALTH

By: _____

Name: _____

Title: _____

Date: _____

VENDOR

By: _____

Name: _____

Title: _____

Date: _____
