

## BUSINESS ASSOCIATE AGREEMENT

This Agreement is made and entered into as of \_\_\_\_\_ (the "Effective Date") by and between the hospital(s) listed in **Attachment A** (whether single or multiple, hereafter, "Covered Entity") and the Hospital Quality Institute, a tax-exempt organization formed collectively by various hospital associations, having its principal place of business at 1215 K Street, Suite 800, Sacramento, California 95814 ("Business Associate").

WHEREAS, reference is made to the Service Agreement between Covered Entity and Business Associate dated \_\_\_\_\_, as may be amended from time to time (the "Service Agreement"), pursuant to which Business Associate performs certain activities or functions on behalf of Covered Entity which may include quality and health services analyses and may involve Business Associate's access to Protected Health Information, as hereinafter defined;

WHEREAS, Covered Entity and Business Associate desire to protect the privacy and security of such Protected Health Information (as hereinafter defined) as required by state and federal law, including but not limited to the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 and the Health Information Technology for Economic and Clinical Health Act, Public Law 111-05, and regulations promulgated, or to be promulgated, thereunder (collectively "HIPAA"), as may be amended from time to time;

WHEREAS, in order for Covered Entity and Business Associate to comply with HIPAA, Business Associate must agree to certain provisions designed to preserve the privacy and security of Protected Health Information obtained by Business Associate in the course of providing services to or on behalf of Covered Entity;

WHEREAS, when applicable, Covered Entity must comply with the Federal Confidentiality of Alcohol and Drug Abuse Patient Records law and regulations, 42 USC §290dd-2 and 42 CFR Part 2 (collectively, "Part 2"); and

WHEREAS, Business Associate is also a Qualified Service Organization ("QSO") under Part 2 and must agree to certain mandatory provisions regarding the use and disclosure of substance abuse treatment information.

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

1. Compliance with Law. In providing services under the Service Agreement and hereunder, Business Associate shall ensure that it acts in compliance with all applicable federal and state laws and regulations including, without limitation, HIPAA, as in effect or as amended, and, if applicable, the Confidentiality of Medical Information Act (Cal. Civ. Code § 56, et seq.).
2. Definitions. For the purposes of this Agreement, the following terms shall have the following meanings:
  - 2.1. *Breach*. "Breach" shall have the same meaning as the term "breach" in 45 C.F.R. § 164.402, as in effect or as amended.

- 2.2. *Electronic Protected Health Information.* “Electronic Protected Health Information” (EPHI) shall have the same meaning as the term “electronic protected health information” in 45 C.F.R. § 160.103, as in effect or as amended.
- 2.3. *PHI.* “*PHP*” shall mean PHI created or received by Business Associate from or on behalf of Covered Entity.
- 2.4. *Individual.* “Individual” shall have the same meaning as the term "individual" in 45 C.F.R. § 160.103 as in effect or as amended, and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g), as in effect or as amended.
- 2.5. *Personal Information.* “Personal Information” shall mean a patient’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that “Personal information” does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.
- 2.6. *Privacy and Security Rule.* “Privacy and Security Rule” shall mean the Security Standards for the Protection of Electronic Protected Health Information and the Standards for Privacy of Individually Identifiable Health Information set forth at 45 C.F.R. part 160 and part 164, as in effect or as amended.
- 2.7. *Protected Health Information.* “Protected Health Information” or “PHI” shall have the same meaning as the term “protected health information” in 45 C.F.R. §160.103, as in effect or as amended. Also, PHI shall include the term “patient identifying information” under the Confidentiality of Substance Use Disorder Patient Records at 42 C.F.R. § 2.11. For the purposes of this Agreement, PHI and EPHI are collectively referred to as “PHI,” unless otherwise specified.
- 2.8. *Secretary.* “Secretary” shall mean the Secretary of the Department of Health and Human Services or his or her designee.
- 2.9. *Security Incident.* “Security Incident” shall mean the successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

All other capitalized terms used in this Agreement but not otherwise defined will have the same meaning as those terms in the Privacy and Security Rule.

### 3. Permitted Uses and Disclosures.

- 3.1. Business Associate may use or disclose PHI only as permitted or required by this Agreement or as required by law. To the extent Business Associate carries out any of Covered Entity’s obligations under HIPAA, Business Associate shall comply with the requirements of HIPAA that apply to Covered Entity in the performance of such obligations.

- 3.2. Business Associate may use or disclose PHI for the following purposes only:
- (a) To fulfill its obligations under the Service Agreement and this Agreement;
  - (b) If necessary, for its proper management and administration or to carry out its legal responsibilities. Disclosure pursuant to this Section 3.2(b) is permissible only if
    - (i) the disclosure is Required by Law; or
    - (ii) Business Associate makes the disclosure pursuant to an agreement consistent with Section 8 of this Agreement or Business Associate makes the disclosure pursuant to a written confidentiality agreement under which the recipient of the PHI is required to (1) protect the confidentiality of the PHI, (2) only use or further disclose the PHI as Required by Law or for the purpose for which it was disclosed to the recipient, and (3) notify Business Associate of any acquisition, access, use, or disclosure of PHI in a manner not permitted by the confidentiality agreement.
  - (c) To report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1).
  - (d) To create one or more limited data sets and disclose such limited data set(s) to the California Hospital Association or one of its affiliates in accordance with 45 C.F.R. § 164.514(e) and in accordance with the applicable data use agreement between and among those parties.
- 3.3. Business Associate shall not, and shall assure that its employees, other agents and contractors do not, use or disclose PHI in any manner which would violate the Privacy and Security Rule if so used or disclosed by Covered Entity.
- 3.4. Business Associate shall, to the extent required by the “minimum necessary” requirements of HIPAA, request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure. To the extent practicable, Business Associate shall not request, use or disclose any Direct Identifiers (as defined in the limited data set standard of HIPAA) and shall comply with the minimum necessary guidance to be issued by the Secretary pursuant to the Health Information Technology for Economic and Clinical Health Act, Public Law 111-05.
4. Safeguarding PHI. Business Associate shall comply with the HIPAA Security Rule with respect to EPHI. Business Associate agrees that it will use appropriate safeguards to prevent the use or disclosure of PHI in a manner contrary to the terms and conditions of this Agreement and will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of EPHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity. Such safeguards shall include, but not be limited to those required by applicable law, including, but not limited to, the Privacy and Security Rule. Business Associate shall ensure that: only those employees and agents of Business Associate that have a business need to know PHI are provided with access to it; access is limited to the minimum amount necessary to accomplish the intended purpose of the access; all employees and agents of Business Associate handling PHI are educated on how to maintain its

confidentiality and the requirements of this Agreement; and all PHI is stored and transmitted in a secure environment and in a manner that prevents its inadvertent disclosure.

5. Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure, including a Breach, of PHI by Business Associate in violation of this Agreement or HIPAA.
6. Reporting Requirements.
  - 6.1. Business Associate shall, without unreasonable delay, but in no event later than five (5) business days after becoming aware of any acquisition, access, use, or disclosure of Protected Health Information in violation of this Agreement by Business Associate, its employees, other agents or contractors or by a third party to which Business Associate disclosed PHI (each, an "Unauthorized Use or Disclosure"), report such use or disclosure, in writing, to Covered Entity. Without limiting the foregoing, Business Associate shall report to Covered Entity any acquisition, access, use, or disclosure that is potentially reportable under Sections 6.1-6.4 of this Agreement, even if it determines that there is a low probability that the PHI or Personal Information, as applicable, has been compromised.
  - 6.2. Business Associate shall, without unreasonable delay, but in no event later than five (5) business days after becoming aware of any Security Incident report it, in writing, to Covered Entity.
  - 6.3. Business Associate shall, without unreasonable delay, but in no event later than five (5) business days after becoming aware of an Unauthorized Use or Disclosure(whether secure or unsecured), report such Breach, in writing, to Covered Entity in accordance with 45 C.F.R. § 164.410.
  - 6.4. Business Associate shall, without unreasonable delay, but in no event later than five (5) business days after becoming aware of a Security Incident report such Breach of Security, in writing to Covered Entity.
  - 6.5. Subject to limitations on damages and indemnity obligations in the Service Agreement, Business Associate shall reimburse Covered Entity for all costs, expenses (including reasonable attorneys' fees), damages and other losses resulting from any breach of this Agreement, Unauthorized Use or Disclosure, Security Incident, or Breach involving Protected Health Information and/or Personal Information maintained by Business Associate, including, without limitation: fines or settlement amounts owed to a state or federal government agency; the cost of any notifications to Individuals or government agencies; credit monitoring for affected Individuals; or other mitigation steps taken by Covered Entity to comply with HIPAA or state law.
7. Personal Information. To the extent that Business Associate has access to Personal Information, Business Associate agrees that it has implemented and maintains appropriate security measures for the protection of Personal Information in accordance with HIPAA or state law.
8. Subcontractors. Business Associate shall enter into a written agreement meeting the requirements of 45 C.F.R. §§ 164.504(e) and 164.314(a)(2) with each Subcontractor (including, without limitation, a Subcontractor that is an agent under applicable law) that creates, receives, maintains or transmits Protected Health Information on behalf of Business Associate. Business Associate

shall ensure that the written agreement with each Subcontractor does the following: (a) obligates the Subcontractor to comply with restrictions and conditions that are at least as restrictive as the restrictions and conditions that apply to Business Associate under this Agreement; and (b) prohibits Subcontractor from sharing with Business Associate the raw data files provided to Subcontractor by Covered Entity.

9. Access to PHI. At the request of Covered Entity, Business Associate shall provide access to PHI in a Designated Record Set as directed by Covered Entity, to an Individual in order to meet the requirements of 45 C.F.R. § 164.524. Covered Entity shall designate the time and manner in which this requirement must be met at the time of the request.
10. Amendment of PHI. Business Associate shall provide to Covered Entity any PHI in a Designated Record Set requested by Covered Entity for amendment as required by 45 C.F.R. § 164.526 within ten (10) days of receipt of such request. Business Associate shall make any amendments to PHI as directed by Covered Entity within thirty (30) days of Covered Entity's request for such amendment, and shall notify Covered Entity, in writing, when such amendment has been completed.
11. Audit and Inspection of Records. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity to Covered Entity, or to the Secretary, in a time and manner designated by Covered Entity or the Secretary, for purposes of the Secretary's determining Covered Entity's and/or Business Associate's compliance with the Privacy and Security Rule. Business Associate shall cooperate with the Secretary if the Secretary undertakes an investigation or other review to determine Covered Entity's or Business Associate's compliance with the Privacy and Security Rule, and shall retain any and all such records, and submit such compliance reports, as may be required by the Secretary or the Privacy and Security Rule.
12. Documentation of Disclosures. Business Associate shall document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528, as in effect or as amended.
13. Accounting of Disclosures. Business Associate shall provide to Covered Entity or an Individual, in a time and manner designated by Covered Entity, such information collected in accordance with Section 12 above to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. Business Associate shall provide, at a minimum, the following information for each disclosure: (a) the date of the disclosure; (b) the name and, if known, address of the entity or person who received PHI; (c) a brief description of PHI disclosed; and (d) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure. Business Associate shall provide information to Covered Entity pursuant to this subsection for all disclosures made within six (6) years prior to the date on which the accounting of disclosures was requested.
14. Ownership of PHI. Business Associate hereby acknowledges that all PHI shall be and remain the sole property of Covered Entity, including any and all forms thereof developed by Business Associate in the course of its fulfillment of its obligations pursuant to this Agreement.
15. Requests for PHI. Business Associate agrees to notify Covered Entity within five (5) business days of Business Associate's receipt of any request, subpoena, or judicial or administrative order

for PHI. To the extent Covered Entity decides to assume responsibility for challenging the validity of such request, Business Associate agrees to cooperate fully with Covered Entity in such challenge.

16. Electronic Data Interchange. To the extent applicable, Business Associate represents and warrants that it shall conduct only as Standard Transactions, as defined in 45 C.F.R. Part 162, any electronic transactions that Business Associate conducts on behalf of a Covered Entity with other Covered Entities or with any entity that requests a transaction be conducted as a Standard Transaction.

17. Obligations of Covered Entity.

17.1. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

17.2. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

17.3. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy and Security Rule if done by Covered Entity, other than as expressly permitted in Sections 3.2(b) and 3.2(c) of this Agreement.

18. Qualified Service Organization.

18.1. To the extent that in performing its services for or on behalf of Covered Entity, Business Associate uses, discloses, maintains, or transmits PHI that is protected by Part 2, Business Associate acknowledges and agrees that it is a QSO for the purpose of such federal law; acknowledges and agrees that in receiving, storing, processing or otherwise dealing with any such patient records, it is fully bound by Part 2; and, if necessary will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by Part 2. This includes the processing of raw data by Business Associate's Vendor as defined in the Service Agreement. Business Associate shall ensure its Vendor is subject to a written agreement that requires Vendor to comply with Part 2 use and disclosure restrictions.

18.2. Notwithstanding any other language in this Agreement, Business Associate acknowledges and agrees that any patient information it receives from Covered Entity that is protected by Part 2 is subject to protections that prohibit Business Associate from disclosing such information to agents or subcontractors without the specific written consent of the subject individual.

18.3. Business Associate acknowledges that any unauthorized disclosure of information under this section is a federal criminal offense.

19. Term and Termination.

19.1. This Agreement shall commence as of the Effective Date, and shall continue in effect until such time as:

- (a) all PHI provided to Business Associate, or created or received by Business Associate on behalf of Covered Entity is destroyed or returned to Covered Entity;
- (b) if it is infeasible to return or destroy PHI, as determined in accordance with Section 20.3 of this Agreement, protections are extended to such PHI in accordance with the terms of this Agreement; or
- (c) the Service Agreement is terminated, subject to the provisions of this Agreement related to the Effect of Termination.

19.2. In the event Business Associate commits a material breach of the terms of this Agreement, Covered Entity may, in its sole discretion, either (a) provide Business Associate with fifteen (15) days to cure such breach, and if Business Associate fails to cure such breach within such period, Covered Entity shall have the right to immediately terminate this Agreement and the Service Agreement; or (b) terminate this Agreement and the Service Agreement immediately, if cure is not possible, as determined by Covered Entity. Termination pursuant to this Section 19.2 shall be without prejudice to any other rights and remedies that Covered Entity may have for a breach of this Agreement. Business Associate acknowledges and agrees that if termination or cure are not feasible, Covered Entity shall report the violation to the Secretary.

20. Effect of Termination.

20.1. Upon the expiration of this Agreement or in the event of the termination of this Agreement for any reason, each party shall be released from all obligations and liabilities to the other under this Agreement and the Service Agreement occurring or arising after the date of such event, except that the expiration or termination of this Agreement shall not relieve Business Associate of Business Associate's obligations under this Section 20, nor shall it relieve Business Associate or Covered Entity Health from any liability arising from any breach of this Agreement. The Service Agreement shall also terminate concurrently with the termination or expiration of this Agreement, subject to the survival provisions of that Service Agreement.

20.2. Immediately upon expiration or termination of this Agreement for any reason, Business Associate shall return, or at Covered Entity's request destroy, all PHI in its possession without retaining copies thereof, and shall provide to Covered Entity upon request a certificate as to the return or destruction of such PHI. Business Associate shall also be responsible for ensuring the return or destruction of PHI in the possession of Business Associate's subcontractors or agents in accordance with this Section.

20.3. In the event that Business Associate determines that returning or destroying PHI is infeasible, Business Associate shall provide to Covered Entity written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

21. Insurance. Business Associate shall procure and maintain during the term of this Agreement liability insurance in accordance with the Service Agreement. Business Associate shall notify

Covered Entity immediately in the event of a lapse, cancellation, or material modification of such coverage as provided in the Service Agreement.

- 22. Injunction. Business Associate hereby agrees that Covered Entity will suffer irreparable damage upon Business Associate's breach of this Agreement, and that such damages shall be difficult to quantify. Business Associate hereby agrees that Covered Entity may seek an injunction to enforce the terms of this Agreement against Business Associate, in addition to any other remedy that they may have.
- 23. Relationship of the Parties. It is expressly understood that Business Associate and Business Associate's employees and agents, if any, are not agents or employees of Covered Entity and have no authority whatsoever to bind Covered Entity, by contract or otherwise.
- 24. Third Party Beneficiaries. Nothing expressed or implied in this Agreement is intended to confer, not shall anything herein confer, upon any person or entity other than the parties hereto any rights, remedies, obligations or liabilities whatsoever.
- 25. Survival. Notwithstanding anything in this Agreement to the contrary, the provisions of Section 18 shall survive the termination of this Agreement and any existing agreement, including the Service Agreement between Covered Entity and Business Associate.
- 26. Notice. Any notice to the other party pursuant to this Agreement shall be deemed provided if sent by first class United States mail, postage prepaid, as follows:

To Covered Entity: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

with a copy to: Chief Legal Officer (at the same address)

To Business Associate: Hospital Quality Institute  
1215 K Street, Suite 800  
Sacramento, California 95814

The above addresses may be changed by giving notice of such change in the manner set forth in this Section.

- 27. 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 HIPAA or other applicable law; provided, however, that any regulations applicable to Business Associate or to Covered Entity with respect to Business Associate promulgated following the Effective Date of this Agreement shall be deemed incorporated into this Agreement until such time as the parties enter into an appropriate amendment. Covered Entity may terminate this Agreement upon thirty (30) days written notice in the event that Business Associate does not promptly enter into an amendment that Covered Entity, in its sole discretion, deems sufficient to ensure that Covered Entity will be able to comply with HIPAA.
- 28. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with HIPAA or other applicable law.



29. Effect. The terms and provisions of this Agreement shall supersede any other conflicting or inconsistent terms in the Service Agreement. All other terms of the Service Agreement between Covered Entity and Business Associate shall remain in full force and effect.

COVERED ENTITY:

**[Name of Hospital]**

By: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

BUSINESS ASSOCIATE:

**Hospital Quality Institute**

By: \_\_\_\_\_

Name: Robert Imhoff

Title: President

Date: \_\_\_\_\_

**ATTACHMENT A**

Hospital Name	OSHDP ID	CMS CCN	NHSN ID