

ATTACHMENT D
BUSINESS ASSOCIATE CONTRACT

A. GENERAL PROVISIONS AND RECITALS

1. The Parties agree that the terms used, but not otherwise defined below in Paragraph B, shall have the same meaning given to such terms under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (“the HITECH Act”), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (DHHS) (“the HIPAA regulations”) (45 CFR Parts 160, 162 and 164) as they may exist now or be hereafter amended.

2. The Parties agree that a business associate relationship under HIPAA, the HITECH Act, and the HIPAA regulations between the Contractor and County arises to the extent that Contractor performs, or delegates to subcontractors to perform, functions or activities on behalf of County pursuant to, and as set forth in, the Agreement that are described in the definition of “Business Associate” in 45 CFR § 160.103.

3. The County wishes to disclose to Contractor certain information pursuant to the terms of the Agreement, some of which may constitute Protected Health Information (“PHI”), as defined below in Subparagraph B.10, to be used or disclosed in the course of providing services and activities pursuant to, and as set forth, in the Agreement.

4. The Parties intend to protect the privacy and provide for the security of PHI that may be created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement in compliance with the applicable standards, implementation specifications, and requirements of HIPAA, the HITECH Act, and the HIPAA regulations as they may exist now or be hereafter amended.

5. The Parties understand and acknowledge that HIPAA, the HITECH Act, and the HIPAA regulations do not pre-empt any state statutes, rules, or regulations that are not otherwise pre-empted by other Federal law(s) and impose more stringent requirements with respect to privacy of PHI.

6. The Parties understand that the HIPAA Privacy and Security rules, as defined below in Subparagraphs B.9 and B.14, apply to the Contractor in the same manner as they apply to a covered entity (County). Contractor agrees therefore to be in compliance at all times with the terms of this Business Associate Contract and the applicable standards, implementation specifications, and requirements of the Privacy and the Security rules, as they may exist now or be hereafter amended, with respect to PHI and electronic PHI created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement.

B. DEFINITIONS

1. “Administrative Safeguards” are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect

electronic PHI and to manage the conduct of Contractor's workforce in relation to the protection of that information.

2. "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

a. Breach excludes:

i. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of Contractor or County, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

ii. Any inadvertent disclosure by a person who is authorized to access PHI at Contractor to another person authorized to access PHI at the Contractor, or organized health care arrangement in which County participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.

iii. A disclosure of PHI where Contractor or County has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

b. Except as provided in paragraph (a) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless Contractor demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

ii. The unauthorized person who used the PHI or to whom the disclosure was made;

iii. Whether the PHI was actually acquired or viewed; and

iv. The extent to which the risk to the PHI has been mitigated.

3. "Data Aggregation" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.

4. "Designated Record Set" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.

5. "Disclosure" shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

6. "Health Care Operations" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.

7. "Individual" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

8. "Physical Safeguards" are physical measures, policies, and procedures to protect

CONTRACTOR's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

9. "The HIPAA Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

10. "Protected Health Information" or "PHI" shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

11. "Required by Law" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.103.

12. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

13. "Security Incident" means attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. "Security incident" does not include trivial incidents that occur on a daily basis, such as scans, "pings", or unsuccessful attempts to penetrate computer networks or servers maintained by Contractor.

14. "The HIPAA Security Rule" shall mean the Security Standards for the Protection of electronic PHI at 45 CFR Part 160, Part 162, and Part 164, Subparts A and C.

15. "Subcontractor" shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

16. "Technical safeguards" means the technology and the policy and procedures for its use that protect electronic PHI and control access to it.

17. "Unsecured PHI" or "PHI that is unsecured" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued on the HHS Web site –

<http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html> .

18. "Use" shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

C. OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE:

1. Contractor agrees not to use or further disclose PHI County discloses to Contractor other than as permitted or required by this Business Associate Contract or as required by law.

2. Contractor agrees to use appropriate safeguards, as provided for in this Business Associate Contract and the Agreement, to prevent use or disclosure of PHI County discloses to Contractor or Contractor creates, receives, maintains, or transmits on behalf of County other than as provided for by this Business Associate Contract.

3. Contractor agrees to comply with the HIPAA Security Rule at Subpart C of 45 CFR Part 164 with respect to electronic PHI County discloses to Contractor or Contractor creates, receives,

maintains, or transmits on behalf of County.

4. Contractor agrees to mitigate, to the extent practicable, any harmful effect that is known to Contractor of a Use or Disclosure of PHI by Contractor in violation of the requirements of this Business Associate Contract.

5. Contractor agrees to report to County immediately any Use or Disclosure of PHI not provided for by this Business Associate Contract of which Contractor becomes aware. Contractor must report Breaches of Unsecured PHI in accordance with Paragraph E below and as required by 45 CFR § 164.410.

6. Contractor agrees to ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of Contractor agree to the same restrictions and conditions that apply through this Business Associate Contract to Contractor with respect to such information.

7. Contractor agrees to provide access, within fifteen (15) calendar days of receipt of a written request by County, to PHI in a Designated Record Set, to County or, as directed by County, to an Individual in order to meet the requirements under 45 CFR § 164.524.

8. Contractor agrees to make any amendment(s) to PHI in a Designated Record Set that County directs or agrees to pursuant to 45 CFR § 164.526 at the request of County or an Individual, within thirty (30) calendar days of receipt of said request by County. Contractor agrees to notify County in writing no later than ten (10) calendar days after said amendment is completed.

9. Contractor agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Contractor on behalf of, County available to County and the Secretary in a time and manner as determined by County or as designated by the Secretary for purposes of the Secretary determining County's compliance with the HIPAA Privacy Rule.

10. Contractor agrees to document any Disclosures of PHI County discloses to Contractor or Contractor creates, receives, maintains, or transmits on behalf of County, and to make information related to such Disclosures available as would be required for County to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528.

11. Contractor agrees to provide County or an Individual, as directed by County, in a time and manner to be determined by County, that information collected in accordance with the Agreement, in order to permit County to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528.

12. Contractor agrees that to the extent Contractor carries out County's obligation under the HIPAA Privacy and/or Security rules Contractor will comply with the requirements of 45 CFR Part 164 that apply to County in the performance of such obligation.

13. Contractor shall work with County upon notification by Contractor to County of a Breach to properly determine if any Breach exclusions exist as defined in Subparagraph B.2.a above.

D. SECURITY RULE

1. Contractor shall comply with the requirements of 45 CFR § 164.306 and establish and maintain appropriate Administrative, Physical and Technical Safeguards in accordance with 45 CFR § 164.308, § 164.310, § 164.312, and § 164.316 with respect to electronic PHI County discloses to Contractor or Contractor creates, receives, maintains, or transmits on behalf of County. Contractor shall follow generally accepted system security principles and the requirements of the HIPAA Security Rule pertaining to the security of electronic PHI.

2. Contractor shall ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of Contractor agree through a contract with Contractor to the same restrictions and requirements contained in this Paragraph D of this Business Associate Contract.

3. Contractor shall report to County immediately any Security Incident of which it becomes aware. Contractor shall report Breaches of Unsecured PHI in accordance with Paragraph E below and as required by 45 CFR § 164.410.

E. BREACH DISCOVERY AND NOTIFICATION

1. Following the discovery of a Breach of Unsecured PHI , Contractor shall notify County of such Breach, however both Parties agree to a delay in the notification if so advised by a law enforcement official pursuant to 45 CFR § 164.412.

a. A Breach shall be treated as discovered by Contractor as of the first day on which such Breach is known to Contractor or, by exercising reasonable diligence, would have been known to Contractor.

b. Contractor shall be deemed to have knowledge of a Breach, if the Breach is known, or by exercising reasonable diligence would have known, to any person who is an employee, officer, or other agent of Contractor, as determined by federal common law of agency.

2. Contractor shall provide the notification of the Breach immediately to the County Privacy Officer at

<p>Andrew Alipanah, MBA, CISSP Chief Information Security Officer 721 S. Parker St. Suite 200 Orange, CA 92868 Phone: (714) 567-7611 Andrew.Alipanah@ocit.ocgov.com</p>	<p>Linda Le, CHPC, CHC, CHP County Privacy Officer 721 S. Parker St. Suite 200 Orange, CA 92868 Phone: (714) 834-4082 Linda.Le@ocit.ocgov.com</p>
---	---

a. Contractor's notification may be oral, but shall be followed by written notification within 24 hours of the oral notification.

3. Contractor's notification shall include, to the extent possible:

a. The identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Contractor to have been, accessed, acquired, used, or disclosed during the Breach;

b. Any other information that County is required to include in the notification to Individual under 45 CFR §164.404 (c) at the time Contractor is required to notify County or promptly thereafter as this information becomes available, even after the regulatory sixty (60) day period set forth in 45 CFR § 164.410 (b) has elapsed, including:

(1) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

(2) A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(3) Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;

(4) A brief description of what Contractor is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any future Breaches; and

(5) Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

4. County may require Contractor to provide notice to the Individual as required in 45 CFR § 164.404, if it is reasonable to do so under the circumstances, at the sole discretion of the County.

5. In the event that Contractor is responsible for a Breach of Unsecured PHI in violation of the HIPAA Privacy Rule, Contractor shall have the burden of demonstrating that Contractor made all notifications to County consistent with this Paragraph E and as required by the Breach notification regulations, or, in the alternative, that the acquisition, access, use, or disclosure of PHI did not constitute a Breach.

6. Contractor shall maintain documentation of all required notifications of a Breach or its risk assessment under 45 CFR § 164.402 to demonstrate that a Breach did not occur.

7. Contractor shall provide to County all specific and pertinent information about the Breach, including the information listed in Section E.3.b.(1)-(5) above, if not yet provided, to permit County to meet its notification obligations under Subpart D of 45 CFR Part 164 as soon as practicable, but in no event later than fifteen (15) calendar days after Contractor's initial report of the Breach to County pursuant to Subparagraph E.2 above.

8. Contractor shall continue to provide all additional pertinent information about the Breach to

County as it may become available, in reporting increments of five (5) business days after the last report to County. Contractor shall also respond in good faith to any reasonable requests for further information, or follow-up information after report to County, when such request is made by County.

9. Contractor shall bear all expense or other costs associated with the Breach and shall reimburse County for all expenses County incurs in addressing the Breach and consequences thereof, including costs of investigation, notification, remediation, documentation or other costs associated with addressing the Breach.

F. PERMITTED USES AND DISCLOSURES BY CONTRACTOR

1. Contractor may use or further disclose PHI County discloses to Contractor as necessary to perform functions, activities, or services for, or on behalf of, County as specified in the Agreement, provided that such use or Disclosure would not violate the HIPAA Privacy Rule if done by COUNTY except for the specific Uses and Disclosures set forth below.

a. Contractor may use PHI County discloses to Contractor, if necessary, for the proper management and administration of Contractor.

b. Contractor may disclose PHI County discloses to Contractor for the proper management and administration of Contractor or to carry out the legal responsibilities of Contractor, if:

i. The Disclosure is required by law; or

ii. Contractor obtains reasonable assurances from the person to whom the PHI 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 immediately notifies Contractor of any instance of which it is aware in which the confidentiality of the information has been breached.

c. Contractor may use or further disclose PHI County discloses to Contractor to provide Data Aggregation services relating to the Health Care Operations of Contractor.

2. Contractor may use PHI County discloses to Contractor, if necessary, to carry out legal responsibilities of Contractor.

3. Contractor may use and disclose PHI County discloses to Contractor consistent with the minimum necessary policies and procedures of County.

4. Contractor may use or disclose PHI County discloses to Contractor as required by law.

G. OBLIGATIONS OF COUNTY

1. County shall notify Contractor of any limitation(s) in County's notice of privacy practices in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Contractor's Use or Disclosure of PHI.

2. County shall notify Contractor of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect Contractor's Use

or Disclosure of PHI.

3. County shall notify Contractor of any restriction to the Use or Disclosure of PHI that County has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Contractor's Use or Disclosure of PHI.

4. County shall not request Contractor to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by County.

H. BUSINESS ASSOCIATE TERMINATION

1. Upon County's knowledge of a material breach or violation by Contractor of the requirements of this Business Associate Contract, County shall:

a. Provide an opportunity for Contractor to cure the material breach or end the violation within thirty (30) business days; or

b. Immediately terminate the Agreement, if Contractor is unwilling or unable to cure the material breach or end the violation within (30) days, provided termination of the Agreement is feasible.

2. Upon termination of the Agreement, Contractor shall either destroy or return to County all PHI Contractor received from County or Contractor created, maintained, or received on behalf of County in conformity with the HIPAA Privacy Rule.

a. This provision shall apply to all PHI that is in the possession of Subcontractors or agents of Contractor.

b. Contractor shall retain no copies of the PHI.

c. In the event that Contractor determines that returning or destroying the PHI is not feasible, Contractor shall provide to County notification of the conditions that make return or destruction infeasible. Upon determination by County that return or destruction of PHI is infeasible, Contractor shall extend the protections of this Business Associate Contract to such PHI and limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction infeasible, for as long as Contractor maintains such PHI.

3. The obligations of this Business Associate Contract shall survive the termination of the Agreement.