

WARNING: At a CCLHO HIE Toolkit workgroup meeting March 17, 2011, the consensus was that Business Associate Agreements are not used in California. This document is included for informational purposes, since the elements included in this sample agreement may need to be included in a ‘confidential Data sharing Agreement’ or other contract regarding health information exchange.

**COUNTY OF XXXX
HIPAA BUSINESS ASSOCIATE AGREEMENT**

Recitals:

- A. COUNTY, as a “Covered Entity” (defined below) wishes to disclose certain information to CONTRACTOR, hereafter known as the “BUSINESS ASSOCIATE” (defined below) pursuant to the terms of the Agreement, some of which may constitute Protected Health Information (“PHI”) (defined below).
- B. COUNTY and BUSINESS ASSOCIATE intend to protect the privacy and provide for the security of PHI disclosed to BUSINESS ASSOCIATE pursuant to the Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”), the Health Information and 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 (the “HIPAA Regulations”) and other applicable laws.
- C. As part of the HIPAA Regulations, the Privacy Rule and Security Rule (defined below) requires COUNTY to enter into an Agreement containing specific requirements with BUSINESS ASSOCIATE prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(e), and 164.504(e) of the Code of Federal Regulations (“C.F.R”) and contained in this Agreement.

The parties agree as follows:

1. Definitions

- a. **Breach** shall have the meaning given to such term under the HITECH Act [42 U.S.C. Section 17921].
- b. **Business Associate** shall have the meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including, but not limited to, 42 U.S.C. Section 17938 and 45 C.F.R. Section 160.103.
- c. **Covered Entity** shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. Section 160.103.
- d. **Designated Record Set** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501
- e. **Electronic Protected Health Information** means Protected Health Information that is maintained in or transmitted by electronic media.

- f. **Electronic Health Record** shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921.
- g. **Health Care Operations** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.
- h. **Privacy Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.
- i. **Protected Health Information or PHI** means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501. Protected Health Information includes Electronic Protected Health Information [45 C.F.R. Sections 160.103, 164.501].
- j. **Protected Information** shall mean PHI provided by COUNTY to BUSINESS ASSOCIATE or created or received by BUSINESS ASSOCIATE on COUNTY's behalf.
- k. **Security Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.
- l. **Unsecured PHI** shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h).

2. **Obligations of Business Associate**

- a. **Permitted Uses.** BUSINESS ASSOCIATE shall not use Protected Information except for the purpose of performing BUSINESS ASSOCIATE's obligations under the Agreement as permitted under the Agreement. Further, BUSINESS ASSOCIATE shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so used by COUNTY. However, BUSINESS ASSOCIATE may use Protected Information (i) for the proper management and administration of Business Associate, or (ii) to carry out the legal responsibilities of Business Associate [45 C.F.R. Sections 164.504(e)(2)(i), 164.501(e)(2)(ii)(A) and 164.504(e)(4)(i)].
- b. **Permitted Disclosures.** BUSINESS ASSOCIATE shall not disclose Protected Information except for the purpose of performing BUSINESS ASSOCIATE's obligations under the Agreement and as permitted under the Agreement. BUSINESS ASSOCIATE shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so disclosed by COUNTY. If BUSINESS ASSOCIATE discloses Protected Information to a third party, BUSINESS ASSOCIATE must obtain, prior to making any such disclosure, (i) reasonable *written* assurances from such third party that such Protected Information will be held confidential as provided pursuant to this Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written

- agreement from such third party to immediately notify BUSINESS ASSOCIATE of any breaches of confidentiality of the Protected Information, to the extent it has obtained knowledge of such breach [42 U.S.C. Section 17932; 45 C.F.R. Sections 164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)].
- c. **Prohibited Uses and Disclosures.** BUSINESS ASSOCIATE shall not use or disclose Protected Information for fundraising or marketing purposes. BUSINESS ASSOCIATE shall not disclose Protected Information to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which PHI solely relates [42 U.S.C. Section 17935(a)]. BUSINESS ASSOCIATE shall not directly or indirectly receive remuneration in exchange for Protected Information, except with prior written consent of COUNTY and as permitted by the HITECH Act, 42 U.S.C. Section 17935(d)(2); however this prohibition shall not affect payment by COUNTY to BUSINESS ASSOCIATE for services provided pursuant to the Agreement
 - d. **Appropriate Safeguards.** BUSINESS ASSOCIATE shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Information otherwise than as permitted by the Agreement, including, but not limited to, administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Protected Information, in accordance with 45 C.F.R. Sections 164.308, 164.310, and 164.312 [45 C.F.R. Section 164.504(e)(2)(ii)(B); 45 C.F.R. Section 164.308(b)]. BUSINESS ASSOCIATE shall comply with the policies and procedures and documentation requirements of the HIPAA Security Rule, including, but not limited to, 45 C.F.R. Section 164.316. [42 U.S.C. Section 17931].
 - e. **Reporting of Improper Access, Use or Disclosure.** BUSINESS ASSOCIATE shall report to COUNTY *in writing* of any access, use or disclosure of Protected Information not permitted by the Agreement, and any Breach of Unsecured PHI of which it becomes aware without unreasonable delay and in no case later than two (2) business days after discovery [42 U.S.C Section 17921; 45 C.F.R. Section 164.504(e)(2)(ii)(C); 45 C.F.R. Section 164.308(b)].
 - f. **Business Associate's Agents.** BUSINESS ASSOCIATE shall ensure that any agents, including subcontractors, to whom it provides Protected Information, agree *in writing* to the same restrictions and conditions that apply to BUSINESS ASSOCIATE with respect to such PHI and implement the safeguards required by paragraph c above with respect to Electronic PHI [45 C.F.R. Section 164.504(e)(2)(ii)(D); 45 C.F.R. Section 164.308(b)]. BUSINESS ASSOCIATE shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation [45 C.F.R. Sections 164.530(f) and 164.530(e)(1)].
 - g. **Access to Protected Information.** This provision applies only if the BUSINESS ASSOCIATE maintains a designated record set on behalf of the COUNTY. BUSINESS ASSOCIATE shall make Protected Information maintained by BUSINESS ASSOCIATE or its agents or subcontractors in Designated Record Sets available to COUNTY for inspection and copying within ten (10) days of a request by COUNTY to enable COUNTY to fulfill its obligations under the

- Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.524 [45 C.F.R. Section 164.504(e)(2)(ii)(E)]. If BUSINESS ASSOCIATE maintains an Electronic Health Record, BUSINESS ASSOCIATE shall provide such information in electronic format to enable COUNTY to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. Section 17935(e).
- h. **Amendment of PHI.** This provision applies only if the BUSINESS ASSOCIATE maintains a designated record set on behalf of the COUNTY. Within ten (10) days of receipt of a request from COUNTY for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, BUSINESS ASSOCIATE or its agents or subcontractors shall make such Protected Information available to COUNTY for amendment and incorporate any such amendment to enable COUNTY to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.526.
- i. **Accounting Rights.** Within ten (10) days of notice by COUNTY of a request for an accounting of disclosures of Protected Information, BUSINESS ASSOCIATE and its agents or subcontractors shall make available to COUNTY the information required to provide an accounting of disclosures to enable COUNTY to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.528, and the HITECH Act, including, but not limited to 42 U.S.C. Section 17935(c), as determined by COUNTY. BUSINESS ASSOCIATE agrees to implement a process that allows for an accounting to be collected and maintained by BUSINESS ASSOCIATE and its agents or subcontractors for at least six (6) years prior to the request. However, accounting of disclosures from an Electronic Health Record for treatment, payment or health care operations purposes are required to be collected and maintained for only three (3) years prior to the request, and only to the extent that BUSINESS ASSOCIATE maintains an electronic health record and is subject to this requirement. At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure. In the event that the request for an accounting is delivered directly to BUSINESS ASSOCIATE or its agents or subcontractors, BUSINESS ASSOCIATE shall within five (5) days of a request forward it to COUNTY in writing. It shall be COUNTY's responsibility to prepare and deliver any such accounting requested. BUSINESS ASSOCIATE shall not disclose any Protected Information except as set forth in Sections 2.b. of this Business Associate Agreement [45 C.F.R. Sections 164.504(e)(2)(ii)(G) and 165.528]. The provisions of this subparagraph i shall survive the termination of this Agreement.
- j. **Government Access to Records.** BUSINESS ASSOCIATE shall make its internal practices, books and records relating to the use and disclosure of Protected Information available to COUNTY and to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for purposes of determining BUSINESS ASSOCIATE's compliance with the Privacy Rule [45

C.F.R. Section 164.504(e)(2)(ii)(H)]. BUSINESS ASSOCIATE shall provide to COUNTY a copy of any Protected Information that BUSINESS ASSOCIATE provides to the Secretary concurrently with providing such Protected Information to the Secretary.

- k. **Minimum Necessary.** BUSINESS ASSOCIATE (and its agents or subcontractors) shall request, use and disclose only the minimum amount of Protected Information necessary to accomplish the purpose of the request, use or disclosure [42 U.S.C. Section 17935(b); 45 C.F.R. Part 164, 45 C.F.R. Section 164.514(d)(3)]. BUSINESS ASSOCIATE understands and agrees that the definition of “minimum necessary” is in flux and shall keep itself informed of guidance issued by the Secretary of the United States Department of Health and Human Services with respect to what constitutes “minimum necessary.”
- l. **Data Ownership.** BUSINESS ASSOCIATE acknowledges that BUSINESS ASSOCIATE has no ownership rights with respect to the Protected Information.
- m. **Notification of Breach.** During the term of the Agreement, BUSINESS ASSOCIATE shall notify COUNTY without unreasonable delay and in no case later than two (2) business days of any suspected or actual breach of security, intrusion or unauthorized use or disclosure of PHI of which BUSINESS ASSOCIATE becomes aware and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. Such notice shall include, but not be limited to, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BUSINESS ASSOCIATE to have been accessed, acquired, or disclosed during such breach. BUSINESS ASSOCIATE shall provide COUNTY with any other available information that the COUNTY is required to include in notification to the individual under 45 C.F.R. Section 164.404(c) at the time of the notification required by this subparagraph m or promptly thereafter as information becomes available. [45 C.F.R. 164.410]. BUSINESS ASSOCIATE shall take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.
- n. **Breach Pattern or Practice by COUNTY.** Pursuant to 42 U.S.C. Section 17934(b), if the BUSINESS ASSOCIATE knows of a pattern of activity or practice of the COUNTY that constitutes a material breach or violation of the COUNTY’s obligations under the Agreement, the BUSINESS ASSOCIATE must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, the BUSINESS ASSOCIATE must terminate the Agreement or other arrangement if feasible, or if termination is not feasible, report the problem to the Secretary of the United States Department of Health and Human Services. BUSINESS ASSOCIATE shall provide written notice to COUNTY of any pattern of activity or practice of the COUNTY that BUSINESS ASSOCIATE believes constitutes a material breach or violation of the COUNTY’s obligations under the Agreement within five (5) days of discovery and shall meet with COUNTY to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.

3. **Termination**
 - a. **Material Breach.** A breach by BUSINESS ASSOCIATE of any provision of this Business Associate Agreement, as determined by COUNTY, shall constitute a material breach of the Agreement and shall provide grounds for *immediate* termination of the Agreement, any provision in the Agreement to the contrary notwithstanding. [45 C.F.R. Section 164.504(e)(2)(iii)].
 - b. **Effect of Termination.** Upon termination of the Agreement for any reason, BUSINESS ASSOCIATE shall, at the option of COUNTY, return or destroy all Protected Information that BUSINESS ASSOCIATE or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If return or destruction is not feasible, as determined by COUNTY, BUSINESS ASSOCIATE shall continue to extend the protections of Section 2 of this Addendum to such information, and limit further use of such PHI to those purposes that make the return or destruction of such PHI feasible [45 C.F.R. Section 164.504(e)(ii)(2)(I)]. If COUNTY elects destruction of the PHI, BUSINESS ASSOCIATE shall certify in writing to COUNTY that such PHI has been destroyed.
4. **Amendment to Comply with Law.** COUNTY and BUSINESS ASSOCIATE acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of the Business Associate Agreement may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule and other applicable laws relating to the security or confidentiality of PHI. The parties understand and agree that COUNTY must receive satisfactory written assurance from BUSINESS ASSOCIATE that BUSINESS ASSOCIATE will adequately safeguard all Protected Information. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to the Business Associate Agreement embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule or other applicable laws. COUNTY may terminate the Agreement upon thirty (30) days written notice in the event (i) BUSINESS ASSOCIATE does not promptly enter into negotiations to amend this Business Associate Agreement when requested by COUNTY pursuant to this Section or (ii) BUSINESS ASSOCIATE does not enter into an amendment to this Business Associate Agreement providing assurances regarding the safeguarding of PHI that COUNTY, in its sole discretion, deems sufficient to satisfy the standards and requirements of applicable laws.
5. **Survival.** The respective rights and obligations of Business Associate shall survive the termination of the Agreement.
6. **Interpretation.** Any ambiguity in this Business Associate Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act, the Privacy Rule and the Security Rule.

