

SANTA BARBARA COUNTY BOARD AGENDA LETTER



Clerk of the Board of Supervisors
105 E. Anapamu Street, Suite 407
Santa Barbara, CA 93101
(805) 568-2240

Agenda Number:
Prepared on: 2/14/05
Department Name: General Services
Department No.:
Agenda Date: 3/15/05
Placement: Administrative
Estimate Time: 5 minutes
Continued Item: NO
If Yes, date from:

TO: Board of Supervisors

FROM: Ron Cortez, Director
General Services

STAFF Ken Layman
CONTACT: County HIPAA Compliance Officer - ext: 2603

SUBJECT: Health Insurance Portability and Accountability Act (HIPAA) - Business Associate Agreement Amendment

Recommendation(s):

That the Board of Supervisors:

1. Approve the attached model language for Business Associate Agreements, which incorporates the requirements of the HIPAA Security Rule.
2. Delegate to County Department Heads and the Purchasing Manager, the authority to renegotiate existing County contracts with HIPAA business associates, by incorporating the attached model language, or alternative language which is in substantial conformity with the attached model language.
3. Approve the use of the attached model language in future business associate agreements.

Alignment with Board Strategic Plan:

The recommendation(s) are primarily aligned with actions required by law or by routine business necessity.

Executive Summary and Discussion:

HIPAA is Federal legislation (P.L. 104-191) that was adopted in 1996 and has staggered implementation deadlines. HIPAA is intended to improve the portability and continuity of health insurance coverage; to combat waste, fraud and abuse in health insurance and health care delivery; to improve access to services and coverage; and to simplify the administration of health insurance. The requirements apply specifically to entities considered to be a Health Plan, Healthcare Clearinghouse, Healthcare Provider or Business Associate as defined by HIPAA.

Board of Supervisors
HIPAA

Santa Barbara County is required to comply with HIPAA, because the County is a healthcare provider and is a sponsor of four health plans. The County is characterized as a “Hybrid Entity”, since not all of its functions are required to comply with HIPAA. There are three components of HIPAA – Privacy (establishes requirements for the handling of certain health care information to ensure privacy of patient health care data); Electronic Health Care Transactions and Code Sets (imposes national standardization); and Security (establishes requirements to ensure the security of patient health care information that is in an electronic format). The compliance deadline for the Privacy Rule was April 14, 2003, the deadline for the Transactions and Code Sets Rule was October 16, 2003, and the deadline for the Security rule is April 21, 2005.

The Privacy Rule requires the County to implement a number of safeguards to ensure privacy of patient health care data, including the requirement to enter into “business associate agreements” with certain entities that contract with the County and handle individually identifiable health information, referred to as Protected Health Information (“PHI”). A “business associate agreement” obligates contractors to also comply with the Privacy Rule, if they handle PHI on behalf of the County. The County has negotiated business associate agreements with applicable contracting entities for all contracts entered into after April 14, 2003.¹ For the most part, the business associate agreements entered into with County contractors have utilized a standard business associate agreement that your Board approved in 2003.

With the upcoming compliance deadline of April 21, 2005 for the Security Rule, it is necessary to amend the County’s existing business associate agreements to incorporate the requirements for handling electronic protected health information (“E PHI”).

The Security Rule applies only to PHI in electronic form and, unlike the Privacy Rule, does not cover paper copies of documents or oral information. However, the standards established in the Security Rule are necessarily intertwined with the requirements of the Privacy Rule. Specifically, the Privacy Rule requires the use of reasonable administrative, physical and technical safeguards to protect privacy, and the new Security Rule provides guidance for interpreting the reasonableness of such safeguards.

The Center for Medicare and Medicaid Services (CMS) has been designated as the responsible agency for overseeing compliance and complaints related to the Security Rule.

Generally, the Security Rule requires a covered entity to:

- Ensure the confidentiality, integrity, and availability of all EPHI the covered entity creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule; and

¹ Additionally, affected agreements entered into or modified between October 16, 2002 and April 14, 2003, were amended to include a “business associates agreement”.

Board of Supervisors
HIPAA

- Ensure compliance by its workforce.

The attached model language for a business associate agreement incorporates the Security Rule requirements into the County's existing standard business associate agreement. To facilitate Security Rule compliance, by the April 21, 2005 implementation deadline, it is requested that your Board approve the utilization of the model language and delegate to the Department Heads and the Purchasing Manager the authority to amend this language into existing business associate agreements.

An attempt will be made to use the attached model language in each contract amendment. However, if a contractor is unwilling to accept the attached model language, it is requested that the Department Heads and the Purchasing Manager be delegated the authority to approve alternative language, which is in substantial conformity with the attached model language and approved by County Counsel.

Approval is also sought to use the attached model language in future County contracts, which require business associate agreements.

Mandates and Service Levels:

The County is mandated to comply with the provisions of HIPAA. The Federal Privacy Rule (45 C.F.R. ¶ 164.530 a) requires a covered provider to designate a privacy official for training and the development and implementation of its policies and procedures. In addition, a provider is required to identify a contact person who is responsible for receiving complaints. (45 C.F.R. ¶ 164.530 b). The Federal Security Rule outlines the organizational requirements for a hybrid entity as defined in (45 C.F. R. ¶ 164.105) and requirements for the development of policy and procedures. (45 C.F.R. ¶164.316) April 21, 2005 is the compliance date for the initial implementation of the security standards.

Fiscal and Facilities Impacts:

HIPAA is an unfunded Federal mandate. The General Services department deleted a vacant position in 2003 and added the County HIPAA Privacy Officer position, thus not increasing the number of positions for the Department. Ken Layman was hired as the Privacy Officer on April 14, 2003 to fill this position. The Security Rule states that a HIPAA Security Officer needs to be designated for the entity and this role was added to the Privacy Officer roles and a job description change was developed by the Human Resources Department and presented in a board letter to re-title the job classification. The corresponding resolution was adopted on December 6th. The new title is the County HIPAA Compliance Officer. The budget for this project has been funded in Fiscal 03/04 and Fiscal 04/05 by the 10 departments that are affected by the HIPAA regulations. A new cost center was recently created (1020) for the HIPAA program, Fund 0001 in the General Services Department to track the actual costs. The current budget allocation will be allocated differently in the 06/07 fiscal year, as determined by a HIPAA Steering Committee. The total estimated budget for the 05/06 budget year is \$129,194.

Special Instructions:

Concurrence:

**Amendment to Agreement Between
County of Santa Barbara
and
(Insert Name of Contractor)**

HIPAA Business Associate Amendment

Recitals

- A. On _____, the County of Santa Barbara ("Hybrid Entity") entered into an agreement with _____ ("Contractor") for _____ (if applicable insert Board Contract Number)("Agreement").
- B. The parties acknowledge that the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. 1320d et seq., and its implementing regulations, mandate them to enter into a business associate agreement in order to safeguard protected health information that may be accessed during the performance of the Agreement. The parties acknowledge further that if Contractor creates, receives, maintains or transmits "electronic protected health information", then the HIPAA Security Rule covers it. The HIPAA Security Rule implementation date is April 21, 2005.
- C. The parties intend to amend the Agreement by adding the following business associate terms incorporating the Security Rule.

NOW, THEREFORE, in consideration of the mutual covenants and conditions contained herein, the parties agree to amend the above referenced Agreement to read as follows:

30. **BUSINESS ASSOCIATE.** The County is considered to be a "Hybrid Entity" under the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. 1320d et seq. and its implementing regulations including but not limited to 45 Code of Federal Regulations parts 142, 160, 162, and 164, ("Privacy Rule and Security Rule"). The Contractor is considered to be a "Business Associate" under the Privacy Rule. Contractor must also comply with the Security Rule as a Business Associate, if under this Agreement; it receives, maintains or transmits any health information in electronic form in connection with a transaction covered by part 162 of title 45 of the Code of Federal Regulations.

The County and Contractor acknowledge that HIPAA mandates them to enter into a business associate agreement in order to safeguard protected health information that may be accessed during the performance of this Agreement. The parties agree to the terms and conditions set forth in Exhibit E - HIPAA Business Associate Agreement.

Paragraph #30 and Exhibit E should only be included when a business associate is involved:

Exhibit E

HIPAA Business Associate Agreement

1. Use and Disclosure of Protected Health Information

Except as otherwise provided in this Exhibit, the Contractor may use or disclose protected health information (“PHI”)¹ to perform functions, activities or services for or on behalf of the County, as specified in the underlying agreement, provided that such use or disclosure does not violate HIPAA or other law. The uses and disclosures of PHI may not exceed the limitations applicable to the County under the regulations except as authorized for management, administrative or legal responsibilities of the Contractor. PHI includes without limitation “Electronic Protected Health Information” (“EPHI”)².

2. Further Disclosure of PHI

The Contractor shall not use or further disclose PHI other than as permitted or required by the underlying Agreement, or as required by law.

3. Safeguarding PHI

The Contractor shall use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the underlying Agreement. Contractor shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of EPHI that Contractor creates, receives, maintains or transmits on behalf of County. The actions taken by the Contractor to safeguard EPHI shall include, but may not be limited to:

- a. Encrypting EPHI that it stores and transmits;
- b. Implementing strong access controls, including physical locks, firewalls, and strong passwords;
- c. Using antivirus software that is upgraded regularly;
- d. Adopting contingency planning policies and procedures, including data backup and disaster recovery plans; and
- e. Conducting periodic security training.

¹ “Protected Health Information” means individually identifiable health information including, without limitation, all information, data, documentation and materials, including without limitation, demographic, medical and financial information, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and 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.

² “Electronic Protected Health Information” means Protected Health Information, which is transmitted by Electronic Media (as defined in the HIPAA Security and Privacy Rule) or maintained in Electronic Media.

4. Unauthorized Use or Disclosure of PHI

The Contractor shall report to the County any use or disclosure of the PHI not provided for by the underlying Agreement or otherwise in violation of the Privacy Rule or Security Rule. Contractor shall report to County any security incidents within 10days of becoming aware of such incidents. For purposes of this paragraph, "security incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.

5. Agents and Subcontractors of the Business Associate

The Contractor shall ensure that any agent, including a subcontractor, to which the Contractor provides PHI received from, or created or received by the Contractor on behalf of the County, shall comply with the same restrictions and conditions that apply through the underlying Agreement to the Contractor with respect to such information. The Contractor shall ensure that any agent to whom it provides PHI, including a subcontractor, agrees to implement reasonable and appropriate safeguards to protect such PHI. Contractor shall not use subcontractors or agents, unless it receives prior written consent from County.

6. Access to PHI

At the request of the County, and in the time and manner designated by the County, the Contractor shall provide access to PHI in a Designated Record Set to an Individual or the County to meet the requirements of 45 Code of Federal Regulations section 164.524.

7. Amendments to Designated Record Sets

The Contractor shall make any amendment(s) to PHI in a Designated Record Set that the County directs or at the request of the Individual, and in the time and manner designated by the County in accordance with 45 Code of Federal Regulations section 164.526.

8. Documentation of Uses and Disclosures

The Contractor shall document such disclosures of PHI and information related to such disclosures as would be required for the County to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 Code of Federal Regulations section 164.528. Contractor agrees to implement a process that allows for an accounting to be collected and maintained by Contractor and its agents or subcontractors for at least six years prior to the request, but not before the compliance date of the Privacy Rule.

9. Accounting of Disclosure

The Contractor shall provide to the County or an Individual, in the time and manner designated by the County, information collected in accordance with 45 Code of Federal Regulations section 164.528, to permit the County to respond to a request by the Individual for an accounting of disclosures of PHI in accordance with 45 Code of Federal Regulations section 164.528.

10. Records Available to Covered Entity and Secretary

The Contractor shall make available records related to the use, disclosure, security and privacy protection of PHI received from the County, or created or received by the Contractor on behalf of the County, to the County or to the Secretary of the United State Department of Health and Human Services for purposes of investigating or auditing the County's compliance with the HIPAA privacy and security regulations, in the time and manner designated by the County or the Secretary.

11. Destruction of PHI

a. Upon termination of the underlying Agreement for any reason, the Contractor shall:

- (1) Return all PHI received from the County, or created or received by the Contractor on behalf of the County required to be retained by the Privacy Rule; or
- (2) Return or destroy all other PHI received from the County, or created or received by the Contractor on behalf of the County.

This provision also shall apply to PHI in possession of subcontractors or agents of the Contractor. The Contractor, its agents or subcontractors shall retain no copies of the PHI. However, Contractor, its agents or subcontractors shall retain all protected information throughout the term of the underlying Agreement and shall continue to maintain the information required under Section 8 of this Exhibit for a period of six years after termination of the underlying Agreement.

b. In the event the Contractor determines that returning or destroying the PHI is not feasible, the Contractor shall provide the County notification of the conditions that make return or destruction not feasible. If the County agrees that the return of the PHI is not feasible, the Contractor shall extend the protections of this Exhibit to such PHI and limit further use and disclosures of such PHI for so long as the Contractor, or any of its agents or subcontractors, maintains such PHI.

12. Amendments

The Parties agree to take such action as is necessary to amend the underlying Agreement as necessary for the County to comply with the requirements of the Privacy Rule and its implementing regulations.

13. Mitigation of Disallowed Uses and Disclosures

The Contractor shall mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of PHI by the Contractor in violation of the requirements of the underlying Agreement or the Privacy Rule.

14. Termination of Agreement

The County shall terminate the underlying Agreement upon knowledge of a material breach by the Contractor of which the Contractor fails to cure.

15. Definitions

Terms used, but not otherwise defined, in this Exhibit shall have the same meaning as those in the Privacy Rule.

16. Interpretation

Any ambiguity in this Exhibit shall be resolved to permit County to comply with the Privacy Rule and Security Rule.

All other terms of the Agreement shall remain in effect.

IN WITNESS WHEREOF, the parties have executed this Amendment to be effective on the date executed by the Hybrid Entity.

\
\
\

COUNTY OF SANTA BARBARA
(Insert name of Dept. Head)
(Insert name of Dept.)

CONTRACTOR/BUSINESS ASSOCIATE
(Insert name of Contractor)

By: _____

By: _____
SocSec or TaxID Number:

Date: _____