Yakutat Community Health Center

Privacy 3.0-BUSINESS ASSOCIATE AGREEMENTS
164.308, 164.314, 164.502, 164.504

Issue Date: **12-1-2017**
Effective Date: **12-1-2017**
Responsible for Review: **Chief Compliance Officer**
Scheduled Review Date: **12-1-2019**

Policy:

To establish guidelines for the Yakutat Community Health Center (YCHC) to identify those vendor/business relationships, which meet the HIPAA definition of a "business associate" and provide direction in establishing formalized business associate agreements. YCHC shall implement the required procedures and ensure documentation to establish satisfactory assurance of compliance. HIPAA requirements for business associates are addressed in the following standards:

- 45 CFR § 164.308(b)(1) – HIPAA Security Rule Administrative Safeguards Business Associate Contracts and Other Arrangements
- 45 CFR §164.314 – HIPAA Security Rule Organizational Requirements Business Associate Contracts or Other Arrangements
- 45 CFR § 164.502(e)(1) – HIPAA Privacy Rule Uses and Disclosures of Protected Health Information: General Rules – Disclosures to Business Associates
- 45 CFR §164.504 – HIPAA Privacy Rule Uses and Disclosures: Organizational Requirements

The standards define the concept of a business associate relationship and outline the required elements to be addressed in a business associate agreement (as addressed in this policy).

Responsible for Implementation:

- Chief Compliance Officer
- Administration

Applicable To:

- All Departments/Units Involved with External Business Associates

Key Definitions:

Business Associate (BA): Under the HIPAA Privacy and Security Rules, a person (or entity) who is not a member of the covered entity's workforce and who performs any function or

activity involving the use or disclosure of individually identifiable health information or who provides services to a covered entity that involves the disclosure of individually identifiable health information, such as legal, accounting, consulting, data aggregation, management, accreditation, etc.

Business Associate Agreement (BAA): Under the HIPAA Privacy and Security Rules, a legally binding agreement entered into by a covered entity and BA that establishes permitted and required uses and disclosures of PHI, provides obligations for the BA to safeguard the information and to report any uses or disclosures not provided for in the agreement, and requires the termination of the agreement if there is a material violation. Refer to 45 CFR § 164.502(e)(1) to determine when the standard is not applicable.

Electronic Protected Health Information (EPHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI). Individually identifiable health information that is created by or received by the YCHC, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present or future payment for the provision of health care to an individual.

Procedures:

1) The YCHC shall determine responsible oversight for the management BA relationships and agreements. Responsibility is delegated to the Chief Compliance Officer.

2) The YCHC's departments/business units are responsible for facilitating the assessment of both existing and future vendor/business relationships to determine whether the relationship meets the criteria for a HIPAA BAA. The following criteria define a business associate under HIPAA:

    a) The vendor/business' staff members are not members of the YCHC's workforce.
    b) The vendor/business' is doing something on behalf of the YCHC.
    c) That "something" involves the use and/or disclosure of PHI.
    d) Note that there are certain disclosures to vendors/businesses that do not require establishment of a BAA (see 45 CFR § 164.502(e)(1). These disclosures include:
        i) Disclosures to disclosures by a covered entity to a health care provider concerning the treatment of the individual.
        ii) Disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met.
        iii) Uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the PHI used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with

respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

3) The YCHC may determine the need for BAAs through:
   a) Mapping the flow of PHI and identifying where PHI is used or disclosed or created by external entities.
   b) Reviewing contract management documents/software and identifying where PHI is disclosed to external entities.
   c) Reviewing 1099 tax forms to identify vendors and then identify vendors with business arrangements where PHI is disclosed to external entities or used internally by vendor.
   d) Assessing new vendor/business arrangements to determine if PHI will be used and/or disclosed.

4) When it has been determined that a BA arrangement exits, the department/business unit leader shall contact the responsible individual/team to initiate a BAA document. The department/business unit leader shall provide the following information to "customize" the BAA:
   a) The name and contact information of the BA.
   b) A general description of the type of service being provided by the BA.
   c) Permitted uses and disclosures as applicable to the arrangement (See 6 a).
   d) The name of the organization's department/business unit and leader who established the BAA.
   e) Date of establishment of the BA relationship and BAA.
   f) Name/signature line for the department/business unit leader or Privacy Officer.
   g) Name/signature line for the BA contact.

5) If a vendor/business relationship requiring a BA agreement/addendum is in the process of contract negotiation and development, the provisions of the BAA may be incorporated into the contract as an option (a separate BAA would not be required).

6) Obligations and activities which must be addressed in the BAA document include:

   Privacy Rule Provisions (45 CFR § 164.504(e)(2):

   a) Stated Purposes for Which BA May Use or Disclose PHI: BA is permitted to use and disclose PHI it creates or receives for or from the YCHC for the purposes as described in the addendum. BA may also use PHI it creates or receives for or from the YCHC as minimally necessary for BA's proper management and administration or to carry out BA's legal responsibilities.

   b) Limitations on Use and Disclosure of Protected Health Information: BA agrees it shall not use or disclose, and shall ensure that its directors, officers, employees, contractors and agents do not use or disclose, Protected Health Information for any purpose other than as expressly permitted by the BAA, or required by law, or in any manner that would constitute a violation of the Privacy Standards if used by the organization.

i) The BAA may permit the BA to use and disclose protected health information for the proper management and administration of the BA; and

ii) The BAA may permit the BA to provide data aggregation services relating to the health care operations of the covered entity.

c) Disclosure by Others: To the extent BA is authorized by this Agreement to disclose Protected Health Information to a third party, BA must obtain, prior to making any such disclosure, reasonable assurances from the third party that the Protected Health Information will be held confidential as provided pursuant to the Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and an agreement from the third party to immediately notify BA of any breaches of confidentiality of the PHI, to the extent it has obtained knowledge of such breach.

d) Minimum Necessary: BA shall disclose to its subcontractors, agents or other third parties, and request from the YCHC, only the minimum PHI necessary to performing or fulfilling a specific required or permitted function.

e) Safeguards Against Misuse of Information: BA will establish and maintain all appropriate safeguards to prevent any use or disclosure of PHI other than pursuant to the terms and conditions of the Agreement.

f) Reporting of Disclosures of PHI: BA shall, within 30 days of discovery of any use or disclosure of PHI in violation of the Agreement, report any such use or disclosure to the organization.

g) Agreements by Third Parties: BA shall enter into an agreement with any agent or subcontractor that will have access to PHI that is received from, or created or received by BA on behalf of, the YCHC pursuant to which such agent or subcontractor agrees to be bound by the same restrictions, terms and conditions that apply to BA pursuant to the Agreement with respect to PHI.

h) Access to Information: Within 15 days of a request by the YCHC for access to PHI about an individual contained in a Designated Record Set, BA shall make available to the YCHC the PHI it requests for so long as that information is maintained in the Designated Record Set. If any individual requests access to PHI about the individual directly from BA, BA shall make available and provide a right of access to the PHI to the individual, at the times and in the manner required by the Privacy Standards (see 45 C.F.R. § 164.524, or its successor as it may be amended from time to time). After receiving the request, BA shall notify the organization within 15 days of such request.

i) Availability of PHI for Amendment: BA agrees to make PHI available for amendment and to incorporate any such amendments in the PHI, at the times and in the manner required by the Privacy Standards (see 45 C.F.R. § 164.526 or its successor as it may be amended from time to time).

j) Accounting of Disclosures: Within 30 days of notice by the organization to BA that it has received a request for an accounting of disclosures of PHI regarding an individual during the six years prior to the date on which the accounting was requested, BA shall

make available to the organization such information as is in BA's possession and is required for the organization to make the accounting required by the Privacy Standards (see 45 C.F.R. § 164.528, or its successor as it may be amended from time to time). At a minimum, BA shall provide the organization with the following information: the date of the disclosure; the name of the entity or person who received the PHI, and, if known, the address of such entity or person; a brief description of the PHI disclosed; and a brief statement of the purpose of the disclosure which includes an explanation of the basis for the disclosure. If the request for an accounting is delivered directly to BA, BA shall within 15 days forward the request to the YCHC. The YCHC is responsible for preparing and delivering the accounting requested. BA agrees to implement an appropriate record keeping process to enable it to comply with the requirements of this Section.

k) Availability of Books and Records: BA agrees to make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by BA on behalf of, the YCHC available to the Secretary for purposes of determining the YCHC's and BA's compliance with the Privacy Standards.

l) If the YCHC (covered entity) and the BA are both governmental entities, additional implementation specifications must be addressed (See 45 CFR § 164.504(e)(3).

Security Rule Provisions (45 CFR § 164.314):

m) Implementation of Safeguards: BA agrees to implementation of administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI that it creates, receives, maintains, and transmits on behalf of the YCHC.

n) Agents and Subcontractors: BA agrees that any agent, including a subcontractor, to which the BA provides EPHI, agrees to implement reasonable and appropriate safeguards to protect the EPHI.

o) Security Incidents: BA agrees to report to the YCHC any security incident of which it becomes aware.

p) Termination: BA agreement authorizes termination of the contract by the YCHC, if the YCHC determines that the BA has violated a material term of the contract.

Other Provisions:

q) The YCHC may want to seek legal counsel guidance prior to entering into a BAA that includes language addressing:

   i) Insurance responsibilities.

   ii) Indemnification requirements.

r) If the YCHC chooses to terminate the arrangement with the BA or the BA chooses to terminate the arrangement with the YCHC, the agreement must be terminated as outlined in the provisions of the BAA/addendum or contract.

s) Upon termination or expiration of the business arrangement between the BA and the YCHC, the BA shall either return or destroy all PHI received from the YCHC or created or received by BA on behalf of the YCHC that the BA still maintains in any form as outlined in the provisions of the BAA/addendum or contract.

7) The YCHC does not have a statutory obligation to monitor the activities of its BAs, but does have a statutory responsibility to gain knowledge and assurances of the BAs compliance with the HIPAA Security Rule. The YCHC, however, must respond to reported privacy breaches and security incident events should they occur and take reasonable steps to cure any potential breach or end the violation

8) The YCHC may serve as a BA to another covered entity and may be asked to review and sign that covered entity's external BA agreement/addendum or contract. As a BA, the YCHC should:
   a) Forward the external information to the Privacy Officer to review the submitted BA agreement to ensure that the provisions outlined are consistent with those set forth in this policy or as documented on the attached (See Addendum 2).
   b) If the BA agreement is not consistent with this policy or contains additional provisions or provisions that are inconsistent with the privacy regulation, the Privacy Officer may recommend to the following alternatives.
      (1) Agree to the additional provisions and sign the agreement.
      (2) Refer the agreement to legal counsel to determine appropriateness before signing.
      (3) Refuse to agree to the provisions and notify the covered entity to establish a resolution.

9) To meet the documentation requirements of the Security Rule, the responsible individual/team shall maintain a file/electronic spreadsheet BAAs/addendums/contracts. This file shall include the following information, and shall be available for review as needed:
   a) Date BAA need identified/received by responsible individual/team.
   b) Name of Individual/organization which forwarded the agreement/identified need.
   c) Name of organization for which BAA is needed.
   d) Description of YCHC's operations that the BA is involved with.
   e) Initiation date of original contract (if applicable).
   f) Term of contract.
   g) Date BAA signed by responsible individual.
   h) Location of BAA.
   i) Any additional notes.

10) All BAA documentation shall be maintained for a period of six years beyond the date of when the BAA relationship is terminated.

11) The BAA shall be effective for the length of the relationship between the BA and the YCHC, unless otherwise terminated under the provisions outlined in the agreement.

Applicable Standards/Regulations:

- 45 CFR § 164.308(b)(1) – HIPAA Security Rule Administrative Safeguards Business Associate Contracts and Other Arrangements
- 45 CFR §164.314 – HIPAA Security Rule Organizational Requirements Business Associate Contracts or Other Arrangements
- 45 CFR § 164.502(e)(1) – HIPAA Privacy Rule Uses and Disclosures of Protected Health Information: General Rules – Disclosures to Business Associates
- 45 CFR §164.504 – HIPAA Privacy Rule Uses and Disclosures: Organizational Requirements

APPENDIX 1: EXAMPLES OF BUSINESS ASSOCIATES

EXAMPLES OF BUSINESS ARRANGEMENTS THAT MAY INVOLVE DISCLOSURE OF PHI & REQUIRE BA AGREEMENTS/ADDENDUMS OR CONTRACT PROVISONS

Accrediting/Licensing Agencies (JCAHO)
Accounting Consultants/Vendors
Actuarial Consultants/Vendors
Agents/Contractors Accessing PHI (Consultants)
Application Service Providers (i.e., prescription mgmt.)
Attorneys/Legal Counsel
Auditors
Benchmarking Organizations
Benefit Management Organizations
Claims Processing/Clearinghouse Agency Contracts
Coding Vendor Contracts
Collection Agency Contracts
Computer Hardware Contracts
Computer Software Contracts
Consultants/Consulting Firms
Data Analysis Consultants/Vendors
Data Warehouse Contracts
Emergency Physician Services Contracts
Hospitalist Contracts
Insurance Contracts (Coverage for Risk, Malpractice, etc.)
Interpreter Services Contracts
IT/IS Vendors
Legal Services Contracts
Medical Staff Credentialing Software Contracts
Microfilming Vendor Contracts
Optical Disc Conversion Contracts
Pathology Services Contracts
Paper Recycling Contracts
Patient Satisfaction Survey Contracts
Payer-Provider Contracts (Provider for Health Plan)
Physician Billing Services
Physician Contracts
Practice Management Consultants/Vendors
Professional Services Contracts
Quality Assurance Consultants/Vendors
Radiology Services Contracts
Record Copying Service Vendor Contracts
Record Storage Vendors
Release of Information Service Vendor Contracts
Repair Contractors of Devices Containing PHI
Revenue Enhancement/DRG Optimization Contracts
Risk Management Consulting Vendor Contracts
Shared Service/Joint Venture Contracts with Other Healthcare Organizations
Statement Outsource Vendors
Telemedicine Program contracts
Third Party Administrators
Transcription Vendor Contracts
Waste Disposal Contracts (Hauling, Shredding)

Health Plan Relationships:

Pharmaceutical Benefits Management Contracts

Preauthorization Management Contracts

Case Management Contracts

Third Party Administrator (TPA) Contracts

Wellness Promotion Contracts

AUTHORIZED BY: Rhoda Jensen, Executive Health Director