AHA
Advancing Health in America

Attachment to AHA Legal Advisory

BUSINESS ASSOCIATE AGREEMENT
A Checklist of Required and Optional Provisions

This is a checklist of required and desirable optional elements for business associate agreements that hospitals can use to evaluate how their existing contracts may need to be modified to conform to the latest regulatory requirements imposed by the HIPAA privacy rule. Hospitals also may find this checklist to be a valuable tool in negotiations with vendors who are reluctant to modify existing agreements because they are less knowledgeable about, or entirely unfamiliar with, the contractual elements the HIPAA privacy rule obligates hospitals to include in their agreements.

REQUIRED PROVISIONS

The HIPAA Medical Privacy Rule identifies in § 164.504(e)(2) some required elements that must be present in any Business Associate Agreement. Hospitals must ensure that their Agreements include all of these required provisions.

Does the Business Associate Agreement . . .

- Authorize the Business Associate to make, unless otherwise restricted or limited by the Agreement, any and all uses and disclosures of Protected Health Information (PHI) necessary to perform its obligations under the Agreement?

- Obligate the Business Associate to:

  (a) Use and/or disclose PHI only as permitted or required by the Agreement or required by law?

  (b) Use appropriate safeguards to prevent use or disclosure of PHI other than as permitted or required by the Agreement?

  (c) Report to the hospital any use or disclosure of PHI that is not permitted or required by the Agreement of which it becomes aware?

  (d) Require all its subcontractors and agents that create, receive, use, disclose or have access to PHI to agree, in writing, to the same restrictions and conditions on the use and/or disclosure of PHI that apply to the Business Associate?

  (e) Make available its internal practices, books, and records relating to the use and disclosure of PHI to the Secretary of the Department of Health and Human Services ("HHS") for purposes of determining the hospital's compliance with the HIPAA Medical Privacy Regulation?

(f) Make available, ***in less than 60 days of receiving a written request from the hospital***, information necessary for the hospital to make an accounting of disclosures of PHI about an individual?

(g) Make available, ***in less than 30 days of receiving a written request from the hospital***, PHI necessary for the hospital to respond to individuals' requests for access to PHI about them? **NOTE:** This requirement is necessary when the PHI in the Business Associate's possession constitutes a Designated Record Set.

(h) Incorporate, ***in less than 60 days of receiving a written request from the hospital***, any amendments or corrections to the PHI in accordance with the HIPAA Medical Privacy Regulation? **NOTE:** This requirement is necessary when the PHI in the Business Associate's possession constitutes a Designated Record Set.

(i) If feasible to do so, return to the hospital or destroy, within a specified number of days of the termination or expiration of the Agreement, and retain no copies of, the PHI, including such information in possession of the Business Associate's subcontractors?

NOTE: If return or destruction of the PHI is not feasible, the Agreement must obligate the Business Associate (1) to extend any and all protections, limitations and restrictions contained in the Agreement to its use and/or disclosure of any PHI retained after the termination of the Agreement, and (2) to limit any further uses and/or disclosures to the purposes that make return or destruction of the PHI infeasible. These obligations must survive any termination or expiration of the Agreement.

- Ensure that the hospital may terminate the Agreement if the hospital makes the reasonable determination that the Business Associate has breached a material term of the Agreement?

OPTIONAL PROVISIONS

Although the HIPAA Medical Privacy Rule does not require that the Business Associate Agreement contain the additional provisions indicated below, hospitals might find them beneficial to include for contractual completeness or general contractual and legal purposes. Hospitals, in consultation with their own legal counsel, will need to consider carefully whether, and to what extent, any of these additional provisions serve the interests of the parties to the agreement, as well as, whether the additions are a legally necessary and appropriate part of their business associate agreements. To the extent that any of these provisions are found to be appropriate for the specific relationship involved, hospitals may want to undertake any additional negotiation with a particular business associate that may be necessary to incorporate the additional provisions.

- *Effective Date*. Is each term and condition in the HIPAA compliance section of the Agreement effective on the date the hospital itself must be in compliance with the Privacy Regulation?

- *Definitions.* Does the Agreement . . .

  a. Define all capitalized terms used in the HIPAA compliance section of the Agreement that are not otherwise specifically defined in the Agreement to have a meaning

consistent with the purposes of Title 45 parts 160 through 164 of the United States Code of Federal Regulations, as amended from time to time?

b. Define "PHI" to mean Protected Health Information, as defined in 45 C.F.R. § 164.501, limited to the information received from or created or received on behalf of the hospital?

c. Define "Privacy Regulation" to mean the privacy regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended from time to time?

- *Mitigation.* Does the Agreement obligate the Business Associate to mitigate, to the extent feasible, any harmful effect that is known by the Business Associate of a use or disclosure of PHI by the Business Associate that is in violation of the requirements of the Agreement?

- *Change in Law*. Does the Agreement state that the Parties agree to negotiate to amend the Agreement as necessary to comply with any amendment to any provision of HIPAA or its implementing regulations set forth at 45 C.F.R. parts 160 and 164, including, but not limited to, the Privacy Regulation, which materially alters either Party or both Parties' obligations under the Agreement? That the Parties agree to negotiate in good faith mutually acceptable and appropriate amendment(s) to the Agreement to give effect to such revised obligations? That if the Parties are unable to agree to mutually acceptable amendment(s) within a specified number of days of the relevant change in law or regulations, either Party may terminate the Agreement consistent with its terms?

- *Construction of Terms.* Does the Agreement state that the terms of the HIPAA compliance section of the Agreement shall be construed in light of any applicable interpretation or guidance on HIPAA and/or the Privacy Regulation issued by HHS or the Office of Civil Rights ("OCR") from time to time?

- *No Third Party Beneficiaries.* Does the Agreement state that nothing in the Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever?

- *Permissible Uses and Disclosures by Business Associate.* ***To the extent that the Business Associate will be engaging in any of these permissible activities***, does the Agreement state that, in addition to any other uses and/or disclosures permitted or authorized by this Agreement or required by law, Business Associate may:

  a. Use the PHI in its possession for its proper management and administration and to fulfill any legal responsibilities of the Business Associate?

  b. Disclose the PHI in its possession to a third party for the purpose of the Business Associate's proper management and administration or to fulfill any legal responsibilities of Business Associate when such disclosures are required by law or the Business Associate has received from the third party written assurances that (i) the information will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party; and (ii) the third party will notify the Business Associate of any instances of which it becomes aware in which the confidentiality of the information has been breached?

c. De-identify, as that term is defined in the Privacy Regulation, as currently written or changed from time to time through future amendment, any and all PHI created or received by the Business Associate under the Agreement? **NOTE:** De-identified data is ***not*** the "limited data set" of facially de-identified information-including zip codes, date of birth and dates of service-that may be disclosed for health care operations, public health and research activities under a data use agreement. For data to be truly de-identified, it must be stripped of all the identifiers listed in the rule and the covered entity cannot have *actual knowledge* that the information could be used, alone or in combination with other data, to identify an individual. Such resulting de-identified information would not be subject to the terms of the Section of the Agreement related to HIPAA privacy rule compliance and the Business Associate may use and/or disclose such de-identified information.

- *Responsibilities of Covered Entity.* Does the Covered Entity agree, in regard to the use and/or disclosure of PHI by Business Associate:

    a. To obtain any consent, authorization or permission that may be required by the Privacy Regulation or applicable state laws and/or regulations prior to furnishing the Business Associate the PHI pertaining to an individual?