BAC to the Basics:
Business Associate Contracts Made Easy

Prepared by

Jen C. Salyers

BAC to the Basics:
Business Associate Contracts Made Easy

Table of Contents

BAC to the Basics:
Business Associate Contracts Made Easy

I. Approaches to Creating a Business Associate Contract ("BAC").

a. Determine the kinds of disclosures, uses and types of protected health information ("PHI") that will generally be at issue.

b. Evaluate the risks associated with such disclosures.

c. Consider what is required under HIPAA for the BAC and if there are other protections you need.

d. BAC as a Standalone Agreement.

i. Can cover all the agreements you have with the Business Associate ("BA").

ii. BAC will need to be more inclusive to ensure you have all the protections you need now and may need in the future. For example, the CE may need to give more consideration to what rights it needs in the event of a BA breach of the BAC, or if additional warranties or other protections are needed.

e. BAC as an Addendum.

i. The BAC can be tailored to the specific circumstances of the relationship.

ii. The Covered Entity ("CE") should consider if the underlying agreement to which the BAC serves as an addendum to needs any additional protections included. For example, if a CE generally excludes certain types of contract breaches from the limitation of liability in the underlying agreement, it may want to consider also excluding breaches of the BA's obligations under the BAC.

II. HIPAA Model BAC Provisions.

a. The Model Provisions are nothing more than sample language, and offered only as guidance or a starting point for creating a BAC. The Model Provisions do not form a contract, nor are they intended to be a contract.

b. The Model Provisions cover only the minimal necessary elements of a BAC.

c. The Model Provisions do not address every legal issue that a CE might be concerned about when entering into a BAC. The CE must consider the circumstances surrounding each particular BAC to determine whether other related contractual terms would be appropriate or necessary. For example, the Model Provisions contemplate that each BAC will specify its own particular limitations on use of PHI.

d. **Exhibit A** shows the HIPAA Model Provisions.

III. Mandatory BAC Provisions under HIPAA

a. Section 164.504(e)(2) of HIPAA sets forth the required elements for a BAC. A BAC must do the following:

i. Establish the permitted and required uses and disclosures of PHI by the BA.

ii. Prohibit the BA from further using or disclosing PHI for any purpose other than as permitted in the BAC or as required by law.

iii. Require the BA to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the BAC.

iv. Require the BA to report to the CE any use or disclosure of PHI that is not provided for in the BAC.

v. Require the BA to ensure that any subcontractors and/or agents to whom it provides the PHI agrees to the same restrictions and conditions that apply to the BA.

vi. Require the BA to make PHI available in accordance with Section 164.524.

vii. Require the BA to incorporate any amendments or corrections to PHI when notified by the CE that the information is inaccurate or incomplete in accordance with Section 164.526.

viii. Require BA to make available the information required to provide an accounting of disclosures in accordance with Section 164.528.

ix. Require the BA to make available its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the BA on behalf of, the CE available to the Secretary of HHS for purposes of determining the CE's compliance with the privacy rule.

x. Require the BA, at termination of the BAC, if feasible, to return or destroy all PHI in any form received from, or created or received by the BA on behalf of, the CE that the BA still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the BAC to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

xi. Authorize the CE to terminate the BAC and underlying agreement if the CE determines that the BA has violated a material term of the BAC.

b. **Exhibit B** is a sample BAC that includes only the mandatory provisions.

IV. Optional BAC Provisions under HIPAA

a. Except as otherwise limited in the BAC, the CE may permit the BA to use PHI for the proper management and administration of the BA or to carry out the legal responsibilities of the BA. See 42 CFR 164.504(e)(4)(i).

b. Except as otherwise limited in the BAC, the CE may permit the BA to disclose PHI for the proper management and administration of the BA, provided that disclosures are required by law, or the BA obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the BA of any instances of which it is aware in which the confidentiality of the information has been breached. See 42 CFR 164.504(e)(4)(ii).

c. Except as otherwise limited in the BAC, the CE may permit the BA to use PHI to provide Data Aggregation services to the CE as permitted by 42 CFR 164.504(e)(2)(i)(B).

V. Other Common BAC Provisions

a. Indemnity. The CE may want to include a term providing that the BA will indemnify and hold harmless the CE for any breaches of the BA's obligations under the BAC.

b. Mitigation. The CE may want to create a general contractual obligation for the BA to cooperate with the CE in its efforts to comply with the HIPAA, such as meeting HIPAA reporting requirements or mitigating unlawful disclosures of PHI.

c. Insurance. It may be desirable to require that a party maintain a certain amount of insurance coverage.

d. Notice Provision. While it is not required, it is a good idea to include a notice provision indicating who notices should be sent to and what means of delivery is acceptable.

f. Contract Review. A CE may want the right to review related contracts between BA and their subcontractors to ensure compliance with the BAC.

g. Audit. A CE may want the right to inspect, investigate, and audit the BA for compliance with the BAC.

h. Governing Law. The parties may want to state what state law will govern in the event of a dispute under the BAC.

i. Mutual Warranties and Representations. A party may wish to include any of the following warranties and representations:

i. Each party has the right and authority to enter into this agreement.

ii. Neither execution of the BAC nor a party's performance hereunder will violate or interfere with the terms of another agreement to which it is a party.

iii. Neither party is the subject of voluntary or involuntary petition in bankruptcy.

iv. All such party's employees, agents, representatives whose services may be used to fulfill obligations under the BAC are or shall be appropriately informed of the terms of the BAC.

v. Each party will reasonably cooperate with the other party in performance of the mutual obligations under the BAC.

j. Ownership. State who is the owner of information disclosed under the BAC.

j. Changes in the law. The parties may wish to state that in the event of changes in the law that the parties agree to negotiate amendments to the BAC.

VI. **Exhibit C** is a sample BAC that includes the mandatory provisions, some of the optional and other provisions.

EXHIBIT A
MODEL PROVISIONS

Appendix to the Preamble--Model Business Associate Contract Provisions

Introduction

The Department of Health and Human Services provides these model business associate contract provisions in response to numerous requests for guidance. This is only model language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these model provisions is not required for compliance with the Privacy Rule. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate.

These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement. These provisions only address concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contract under State law and do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this model is not sufficient for compliance with state law and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule. For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet its obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these model provisions. For example, the Privacy Rule does not preclude a business associate from disclosing protected health information to report unlawful conduct in accordance with Sec. 164.502(j). However, there is not a specific model provision related to this permissive disclosure. These and other types of issues will need to be worked out between the parties.

Model Business Associate Contract Provisions

Note:
Words or phrases contained in brackets [ ] are intended as either optional language or as instructions to the users of these model provisions and are not intended to be included in the contractual provisions.

Definitions (alternative approaches)

Catch-all definition:
Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 CFR 160.103 and 164.501.

Examples of specific definitions:

a) Business Associate. ``Business Associate'' shall mean [Insert Name of Business Associate].

b) Covered Entity. ``Covered Entity'' shall mean [Insert Name of Covered Entity].

c) Individual. ``Individual'' shall have the same meaning as the term ``individual'' in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

d) Privacy Rule. ``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.

e) Protected Health Information. ``Protected Health Information'' shall have the same meaning as the term ``protected health information'' in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

f) Required By Law. ``Required By Law'' shall have the same meaning as the term ``required by law'' in 45 CFR 164.501.

g) Secretary. ``Secretary'' shall mean the Secretary of the Department of Health and Human Services or his designee.

Obligations and Activities of Business Associate

a) Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.

b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages by a Business Associate.]

d) Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement.

e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business

Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

f) Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner designated by Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]

g) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity. [Not necessary if business associate does not have protected health information in a designated record set.]

h) Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

i) Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

j) Business Associate agrees to provide to Covered Entity or an Individual, in time and manner designated by Covered Entity, information collected in accordance with Section [Insert Section Number in Contract Where Provision (i) Appears] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

Permitted Uses and Disclosures by Business Associate

<u>General Use and Disclosure Provisions</u> (alternative approaches)

<u>Specify purposes</u>:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity: [List Purposes].

<u>Refer to underlying services agreement</u>:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

a) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

b) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

c) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]

a) Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

b) Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.

c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522.

Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by

Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].

Term and Termination

a) Term. The Term of this Agreement shall be effective as of [Insert Effective Date], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

b) Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the ____ Agreement/ sections ____ of the ____ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, or immediately terminate this Agreement [and the ____ Agreement/sections ____ of the ____ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible. [Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

c) Effect of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(2) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Miscellaneous

a) Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended, and for which compliance is required.

b) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act, Public Law 104-191.

c) Survival. The respective rights and obligations of Business Associate under Section [Insert Section Number Related to ``Effect of Termination"] of this Agreement shall survive the termination of this Agreement.

d) Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule.

EXHIBIT B
SAMPLE BUSINESS ASSOCIATE CONTRACT WITH THE MANDATORY PROVISIONS

Whereas, _____, hereinafter "Covered Entity" and _____, hereinafter "Business Associate," have executed a_____ Agreement effective on _____, 20__, by and between the parties hereto (the "Agreement") and the parties hereto intend to comply with the applicable provisions of the Health Insurance Portability and Accountability Act (1996) ("HIPAA") by executing this document (this "Document") and agreeing to the following:

Business Associate acknowledges and agrees that in the course of performance of Business Associate's obligations under the Agreement, Business Associate might be given or obtain access to information which contains Individually Identifiable Health Information (IIHI). For purposes of this Agreement IIHI has the same meaning as set forth in the regulations promulgated pursuant to 42 U.S.C. Section 1320d, which is any information, including demographic information, collected from an individual that has been received or created by Covered Entity and related 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 identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. Business Associate agrees to receive IIHI from Covered Entity, in order to perform administrative functions on behalf of Covered Entity. Business Associate is providing the following assurances to Covered Entity that the IIHI will be appropriately safeguarded:

1. Business Associate will only use and disclose any IIHI it receives from Covered Entity as is permitted or required under the Agreement between the parties or the law.

2. Business Associate will use appropriate safeguards to prevent the use or disclosure of the IIHI other than as provided for in the Agreement.

3. Business Associate will report to Covered Entity any use or disclosure of IIHI not provided for in the Agreement of which it becomes aware.

4. Business Associate will ensure that any of its agents or subcontractors to whom Business Associate provides Covered Entity's IIHI will agree to the same restrictions and conditions that apply to Business Associate with respect to such IIHI.

5. Business Associate will, upon request, make IIHI available to Covered Entity in accordance with 45 C.F.R. §164.524.

6. Businesses Associate will, upon request, make IIHI available to Covered Entity for amendment and incorporate any amendments in accordance with 45 C.F.R. §164.526.

7. Business Associate will make available the information required to provide an accounting of disclosures in accordance with 45 C.F.R. §164.528.

8. Business Associate will make its internal practices, books, and records relating to the use and disclosure of IIHI received from or created or received by Business Associate on behalf of Covered Entity, available to the Secretary of Health and Human Services (HHS) or any other officer or employee of HHS or other government entity to whom the authority invoked has been

delegated for purposes of determining the Covered Entity's compliance with the privacy regulations promulgated under HIPAA.

9. At termination of the Agreement, Business Associate will, if feasible, return or destroy all IIHI received from or created or received by the Business Associate on behalf of Covered Entity that the Business Associate still maintains in any form and retain no copies of IIHI. If such return or destruction is not feasible, Business Associate will extend the protections of the Agreement to IIHI and limit further uses and disclosures to those purposes that make the return of IIHI infeasible.

10. Business Associate authorizes termination of the Agreement by Covered Entity in the event that Covered Entity determines Business Associate has violated a material term of this Document.

Business Associate	Covered Entity
By _____	By _____
Its_____	Its _____
Date _____	Date_____

EXHIBIT C
SAMPLE HIPAA COMPLIANCE ADDENDUM:
BUSINESS ASSOCIATE, TRADING PARTNER AND CHAIN OF TRUST

THIS ADDENDUM is entered into by and between _____, a _____ corporation ("**BUSINESS ASSOCIATE**") and _____ a _____ corporation ("**COVERED ENTITY**"). The purpose of this Addendum is to satisfy certain obligations of Covered Entity under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 C.F.R. Parts 160-64) ("**HIPAA**") to ensure the integrity and confidentiality of Protected Health Information.

In consideration of the foregoing and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, Business Associate and Covered Entity agree as follows:

1. **Definitions**.[1] Capitalized terms used, but not otherwise defined, in this Addendum shall have the meanings given them in HIPAA. For convenience of reference, the definitions of "Individually Identifiable Health Information" and "Protected Health Information" as of the Effective Date are as follows:

1.1 "**Individually Identifiable Health Information**" means information that is a subset of health information, including demographic information collected from an individual, and (i) is created or received by a healthcare provider, health plan, employer, or health care clearinghouse; and (ii) relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of health care to an individual; and (a) that identifies the individual, or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

1.2 "**Protected Health Information**" means Individually Identifiable Health Information that Business Associate receives from Covered Entity or from another business associate of Covered Entity or which Business Associate creates for Covered Entity which is transmitted or maintained in any form or medium. "Protected Health Information" shall not include education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. §1232g, or records described in 20 U.S.C. §1232g (a)(4)(B)(iv), or employment records held by Covered Entity in its role as employer.

2. **Applicability of Terms; Conflicts.**[2] This Addendum amends the attached agreement (the "Agreement") as of the effective date of the Agreement. In the event of any conflict or inconsistency between a provision of this Addendum and a provision of the Agreement or any other agreement between Business Associate and Covered Entity, the provision of this Addendum shall control unless: (i) Covered Entity specifically agrees to the contrary in writing, or (ii) the provision in the Agreement or such other

[1] While the definitions set forth in HIPAA can simply be referenced, the parties may wish to set forth the definitions for terms that will periodically be referenced in the BAC.

[2] Optional. This section resolves conflicts between the underlying Agreement and the BAC that may arise.

agreement establishes additional rights for Covered Entity or additional duties for or restrictions on Business Associate with respect to Protected Health Information, in which case the provision of the Agreement or such other agreement will control.

3. **Obligations and Activities of Business Associate**

3.1 Business Associate will not use or disclose Protected Health Information other than as permitted or required by this Addendum or as Required By Law or as otherwise authorized by Covered Entity.[3]

3.2 Business Associate will use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Addendum.[4] Business Associate will develop, implement, maintain and use appropriate administrative, technical and physical safeguards to preserve the integrity and confidentiality of and to prevent non-permitted or violating use or disclosure of Protected Health Information which is transmitted electronically. Business Associate will document and keep these safeguards current.[5]

3.3 Business Associate will mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Addendum.[6]

3.4 Business Associate will report to the Privacy Officer of Covered Entity, in writing, any use and/or disclosure of Protected Health Information that is not permitted or required by this Addendum of which Business Associate becomes aware.[7] Such report shall be made as soon as reasonably possible but in no event more than five (5) business days[8] after discovery by Business Associate of such unauthorized use or disclosure. This reporting obligation shall include breaches by Business Associate, its employees, subcontractors and/or agents. Each such report of a breach will: (i) identify the nature of the non-permitted or violating use or disclosure; (ii) identify the Protected Health Information used or disclosed; (iii) identify who made the non-permitted or violating use or disclosure; (iv) identify who received the non-permitted or violating use or disclosure; (v) identify what corrective action Business Associate took or will take to prevent further non-permitted or violating uses or disclosures; (vi) identify what Business Associate did or will do to mitigate any deleterious effect of the non-permitted or violating use or disclosure; and (vii) provide such other information as Covered Entity may reasonably request.[9]

3.5 Business Associate will ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity agrees to the same restrictions and conditions that apply through this Addendum to Business Associate with respect to such information.[10]

3.6 Business Associate will provide access, within five (5) business days of receiving a written request from Covered Entity, to Protected Health Information from a

[3] Addresses concept required under 42 CFR Section 164.504(e)(2)(ii)(A).
[4] Addresses concept required under 42 CFR Section 164.504(e)(2)(ii)(B).
[5] The last two sentences in this section address the chain of trust concept under the proposed HIPAA security rule.
[6] Optional. To the extent the BA is the reason mitigating action is needed, the CE may want the BA to have mitigation responsibilities. The CE may also want to add that the BA mitigate per the CE's instructions.
[7] Addresses concept required under 42 CFR Section 164.504(e)(2)(ii)(C).
[8] Length of time is negotiable.
[9] Consider what information CE will need in the event of a BA breach.
[10] Addresses concept required under 42 CFR Section 164.504(e)(2)(ii)(D).

Designated Record Set of Covered Entity, to Covered Entity (or, as directed by Covered Entity, to an Individual) in order to meet the requirements under 45 C.F.R. § 164.524.[11] This provision does not apply if Business Associate and its employees, subcontractors and agents have no Protected Health Information from a Designated Record Set of Covered Entity.

3.7 Business Associate will make, upon written request from Covered Entity, any amendment(s) to Protected Health Information in a Designated Record Set of Covered Entity that Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526. This provision does not apply if Business Associate and its employees, subcontractors and agents have no Protected Health Information from a Designated Record Set of Covered Entity.[12]

3.8 Business Associate will make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary during regular business hours within five (5) business days of receiving a written request from Covered Entity, or sooner if requested by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with HIPAA.[13]

3.9 Business Associate will document such disclosures by Business Associate and its employees, subcontractors and agents of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R § 164.528. Business Associate agrees to provide to Covered Entity (or an Individual, at Covered Entity's request), within five (5) business days of receiving a written request from Covered Entity, information collected in accordance with the preceding sentence, to permit Covered Entity to respond to a request by an Individual for such an accounting of disclosures.[14]

3.10[15] At Covered Entity's request, Business Associate will implement reasonable alternative means or locations of communication with an Individual, as necessary to honor a request granted by Covered Entity pursuant to 45 C.F.R. §§ 164.522 or 164.526, respectively. Except as the Agreement or any other agreement between Covered Entity and Business Associate may provide otherwise, in the event Business Associate receives an access, amendment, disclosure accounting or confidential communications or other similar request directly from an Individual, Business Associate will redirect the Individual to appropriate Covered Entity personnel. Business Associate will maintain records related to disclosures of Protected Health

[11] Addresses concept required under 42 CFR Section 164.504(e)(2)(ii)(E). Length of time is negotiable. Section 3.6 is only needed if the BA has information that is in the CE's Designated Record Set (DRS). However, a CE may want to keep this section in even if the BA initially has no information in the CE's DRS, because the CE's DRS could change over time.

[12] Addresses concept required under 42 CFR Section 164.504(e)(2)(ii)(F). However, like Section 3.6, this section does not apply if the BA will not have any information in the CE's DRS.

[13] Addresses concept required under 42 CFR Section 164.504(e)(2)(ii)(H). Length of time is negotiable.

[14] BA is required per 42 CFR Section 164.504(e)(2)(ii)(G) to make information available to provide an accounting of disclosures in accordance with 42 CFR 164.528. However, a CE may want to be more specific in this area concerning how quickly the BA needs to respond to CE's request for such information. Some CEs may wish to impose additional reporting requirements of the BA.

[15] Optional provisions.

Information for at least six (6) years after the date of the disclosure.

4. **Permitted Uses and Disclosures by Business Associate.**

4.1 **Functions and Activities on Covered Entity's Behalf.**[16] Except as otherwise limited in this Addendum, the Agreement or any other agreement between Business Associate and Covered Entity, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity only for purposes authorized by Covered Entity in the Agreement or through specific oral instruction[17], if such use or disclosure of Protected Health Information would not violate HIPAA if done by Covered Entity itself.

4.2 **Business Associate's Operations.** Except as otherwise limited in this Addendum, the Agreement or any other agreement between Business Associate and Covered Entity: (a) Business Associate may use Protected Health Information for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities; [18] (b) Business Associate may disclose Protected Health Information for Business Associate's proper management and administration, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the Protected Health Information is disclosed that (i) it will remain confidential and will be used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and (ii) the person will notify Business Associate of any instances of which it is aware in which the confidentiality of the Protected Health Information has been breached.[19]

5. **"Trading Partner" Provisions: Use and Disclosure in Connection with Standard Transactions.**[20] If Business Associate conducts Standard Transactions (as defined in 45 C.F.R. Part 162) for or on behalf of Covered Entity, Business Associate will comply, and will require each subcontractor or agent involved with the conduct of such Standard Transactions to comply, with each applicable requirement of 45 C.F.R. Part 162. Business Associate will not enter into, or permit its subcontractors or agents to enter into, any trading partner agreement in connection with the conduct of Standard Transactions for or on behalf of Covered Entity that: (i) changes the definition, data condition, or use of a data element or segment in a Standard Transaction; (ii) adds any data elements or segments to the maximum defined data set; (iii) uses any code or data element that is marked "not used" in the Standard Transaction's implementation specification or is not in the Standard Transaction's implementation specification; or (iv) changes the meaning or intent of the Standard Transaction's implementation specification.

6. **Term and Termination**

6.1 **Term.** The term of this Addendum shall commence as of the effective date of the Agreement[21], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, for purposes of the Agreement is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such Protected Health Information in

[16] The CE needs to state purposes for which the BA can use and disclose Protected Health Information under 42 CFR Section 164.504(e)(2)(i). HIPAA does not offer any guidance on how specific the stated purposes need to be.

[17] The CE may choose to expand the BA's use of Protected Health Information per specific instruction of the CE (oral or written).

[18] Optional. This language is permitted under 42 CFR Section 164.504(e)(4)(i), but will not be appropriate for every situation.

[19] Optional. This language is permitted under 42 CFR Section 164.504(e)(4)(ii), but will not be appropriate for every situation.

[20] Optional. This language has been included to address the "trading partner" concept under the HIPAA transaction rules.

[21] The effective date is typically the effective date of the underlying Agreement. However, this is negotiable, and, if appropriate, may be based on the date HIPAA's requirement for a BAC goes into effect.

accordance with the provisions of this Section 6.[22]

6.2 **Termination for Cause.** As provided in HIPAA, including 45 C.F.R. §164.504(e)(2)(iii), upon Covered Entity's reasonable determination that Business Associate has breached a material term of this Addendum, Covered Entity shall be entitled to do any one or more of the following:

(a) Give Business Associate written notice of the existence of such breach and give Business Associate an opportunity to cure upon mutually agreeable terms. If Business Associate does not cure the breach or end the violation according to such terms, or if Covered Entity and Business Associate are unable to agree upon such terms, Covered Entity may immediately terminate the Agreement.[23]

(b) Immediately terminate the Agreement.[24]

(c) Immediately stop all further disclosures of Protected Health Information to Business Associate pursuant to the Agreement.[25]

6.3 **Effect of Termination**. Upon receipt of written demand from Covered Entity, Business Associate agrees to immediately return or destroy, except to the extent infeasible, all Protected Health Information demanded by Covered Entity, including all such Protected Health Information which Business Associate has disclosed to its employees, subcontractors and/or agents.[26] Destruction shall include destruction of all copies including backup tapes and other electronic backup medium. In the event the return or destruction of some or all such Protected Health Information is infeasible, Protected Health Information not returned or destroyed pursuant to this paragraph shall be used or disclosed only for those purposes that make return or destruction infeasible.

6.4 **Continuing Privacy Obligation.**[27] Business Associate's obligation to protect the privacy of Protected Health Information is continuous and survives any termination, cancellation, expiration, or other conclusion of this Addendum, the Agreement or any other agreement between Business Associate and Covered Entity.

7. **Notices.**[28] All notices pursuant to this Addendum must be given in writing and shall be effective when received if hand-delivered or upon dispatch if sent by reputable overnight delivery service, facsimile or U.S. Mail to the appropriate address or facsimile number as set forth at the end of this Addendum.

8. **Miscellaneous.** Business Associate and Covered Entity agree that Individuals who are the subject of Protected Health Information are not third-party beneficiaries of this Addendum. In the event that any provision of this Addendum violates any applicable statute, ordinance or rule of law in any jurisdiction that governs this Addendum, such provision shall be ineffective to the extent of such violation without invalidating any other provision of this Addendum. This Addendum may not be amended, altered or modified except by written agreement signed by Business Associate and Covered Entity. No provision of this Addendum may be waived except by an agreement in writing signed by the waiving party. A waiver of any term or provision shall not be construed as a

[22] Addresses concept required under 42 CFR Section 164.504(e)(2)(ii)(I).
[23] Optional.
[24] Optional. Provides additional protection for the CE.
[25] Optional.
[26] Addresses concept required under 42 CFR Section 164.504(e)(2)(ii)(I).
[27] Optional.
[28] Optional.

waiver of any other term or provision. Nothing in Section 3 of this Addendum shall be deemed a waiver of any legally-recognized claim of privilege available to Business Associate. All references herein to specific statutes, codes or regulations shall be deemed to be references to those statutes, codes or regulations as may be amended from time to time.[29]

[29] The foregoing statements in Section 8 are optional.

BUSINESS ASSOCIATE:

_____

By: _____

Its: _____

Address for notices:

_____

Attn: _____
_____
_____

Phone: _____
Fax: _____

COVERED ENTITY:

_____
Officer

By: _____

Its: _____

Address for notices:

Covered Entity's Privacy

Address

Phone: _____
Fax: _____

Copy to:

Covered Entity's Legal Department
Attn: Privacy Notice
Address

Phone: _____
Fax: _____