

BUSINESS ASSOCIATE ADDENDUM (TO BE USED PRIOR TO FEB. 17, 2010)

This form contract is offered for informational purposes only and does not constitute legal advice or a comprehensive guide to issues to be considered in entering into a business associate contract.

This form applies to the relationship between a HIPAA covered entity and its business associate. It complies with legal requirements applicable to business associate contracts prior to Feb. 17, 2010. On Feb. 17, 2010, business associate contracts will be required to comply with additional obligations that are not included in this model document. The Business Associate Addendum (To Be Used After Feb. 17, 2010) complies with those additional requirements.

Optional provisions not required by the HIPAA regulations are highlighted in italics. As an alternative, the provisions of this Addendum may be incorporated directly into the underlying contract.

This Business Associate Addendum (“Addendum”) supplements and is made a part of the contract (“Contract”) by and between Covered Entity (“CE”) and Business Associate (“BA”) dated _____ . This Addendum is effective as of _____ (the “Addendum Effective Date”).

RECITALS

- A. CE wishes to disclose certain information to BA pursuant to the terms of the Contract, some of which may constitute Protected Health Information (“PHI”) (defined below).
- B. CE and BA intend to protect the privacy and provide for the security of PHI disclosed to BA pursuant to the Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”) and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the “HIPAA Regulations”) and other applicable laws.
- C. As part of the HIPAA Regulations, the Privacy Rule and the Security Rule (defined below) require CE to enter into a contract containing specific requirements with BA prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(e) and 164.504(e) of the Code of Federal Regulations (“C.F.R.”) and contained in this Addendum.

In consideration of the mutual promises below and the exchange of information pursuant to this Addendum, the parties agree as follows:

1. Definitions

- a. **Business Associate** shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. Section 160.103.
- b. **Covered Entity** shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. Section 160.103.
- c. **Data Aggregation** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

- d. **Designated Record Set** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

[If the business associate creates, maintains, receives or transmits electronic PHI on behalf of the CE, the following language should be included]: **Electronic Protected Health Information** means Protected Health Information that is maintained in or transmitted by electronic media.

- e. **Health Care Operations** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.
- f. **Privacy Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.
- g. **Protected Health Information or PHI** means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501. *[If the business associate creates maintains, receives or transmits electronic PHI on behalf of the CE, the following language should be included]:* Protected Health Information includes Electronic Protected Health Information.

[45 C.F.R. Sections 160.103, 164.501]
- h. **Protected Information** shall mean PHI provided by CE to BA or created or received by BA on CE's behalf.
- i. **Security Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

2. **Obligations of Business Associate**

- a. **Permitted Uses.** BA shall not use Protected Information except for the purpose of performing BA's obligations under the Contract and as permitted under the Contract and Addendum. Further, BA shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule if so used by CE. However, BA may use Protected Information (i) for the proper management and administration of BA, (ii) to carry out the legal responsibilities of BA, or (iii) for Data Aggregation purposes for the Health Care Operations of CE [45 C.F.R. Sections 164.504(e)(2)(i), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(i)].
- b. **Permitted Disclosures.** BA shall not disclose Protected Information except for the purpose of performing BA's obligations under the Contract and as permitted under the Contract and Addendum. BA shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule if so disclosed by CE. *However, BA may disclose Protected Information (i) for the proper management and administration of BA; (ii) to carry out the legal responsibilities of BA; (iii) as required by law; or (iv) for Data Aggregation purposes for the Health Care Operations of CE.*

If BA discloses Protected Information to a third party, BA must obtain, prior to making any such disclosure, (i) *reasonable* written assurances from such third party that such Protected Information will be held confidential as provided pursuant to this Addendum and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a *written* agreement from such third party to immediately notify BA of any breaches of confidentiality of the Protected Information, to the extent it has obtained knowledge of such breach [45 C.F.R. Sections 164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)].

- c. **Appropriate Safeguards.** BA shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Information otherwise than as permitted by this Contract or Addendum [*If the business associate creates maintains, receives or transmits electronic PHI on behalf of the CE, the following language is required*]: including administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of CE's Electronic Protected Health Information [45 C.F.R. Section 164.504(e)(2)(ii)(B); 45 C.F.R. Section 164.308(b)]. *BA shall maintain a comprehensive written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the BA's operations and the nature and scope of its activities.*
- d. **Reporting of Improper Use or Disclosure.** BA shall report to CE *in writing* of any use or disclosure of Protected Information not permitted by the Contract and Addendum. [*If the business associate creates maintains, receives or transmits electronic PHI on behalf of the CE, the following language is required*]: and any security incident concerning Electronic PHI otherwise than as provided for by the Contract and Addendum of which it becomes aware [*within two (2) days of becoming aware of such use or disclosure*] [45 C.F.R. Section 164.504(e)(2)(ii)(C); 45 C.F.R. Section 164.308(b)].
- e. **Business Associate's Agents.** BA shall ensure that any agents, including subcontractors, to whom it provides Protected Information, agree *in writing* to the same restrictions and conditions that apply to BA with respect to such PHI [*If the business associate creates maintains, receives or transmits electronic PHI on behalf of the CE, the following language is required*]: and implement the safeguards required by paragraph c above with respect to Electronic PHI [45 C.F.R. Section 164.504(e)(2)(ii)(D); 45 C.F.R. Section 164.308(b)]. *BA shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation (see 45 C.F.R. Sections 164.530(f) and 164.530(e)(1)).*
- f. **Access to Protected Information.** [*This provision is required only if the business associate maintains a designated record set on behalf of the covered entity*]: BA shall make Protected Information maintained by BA or its agents or subcontractors in Designated Record Sets available to CE for inspection and copying *within ten (10) days of a request by CE* to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.524 [45 C.F.R. Section 164.504(e)(2)(ii)(E)].
- g. **Amendment of PHI.** [*This provision is required only if the business associate maintains a designated record set on behalf of the covered entity*]: *Within ten (10) days of receipt of a request from CE for an amendment of Protected Information or a record about an individual contained*

in a Designated Record Set, BA or its agents or subcontractors shall make such Protected Information available to CE for amendment and incorporate any such amendment to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.526. If any individual requests an amendment of Protected Information directly from BA or its agents or subcontractors, BA must notify CE in writing within five (5) days of the request. Any approval or denial of amendment of Protected Information maintained by BA or its agents or subcontractors shall be the responsibility of CE [45 C.F.R. Section 164.504(e)(2)(ii)(F)].

- h. Accounting Rights.** *[Within ten (10) days of notice by CE of a request for an accounting of disclosures of Protected Information][Promptly upon any disclosure of Protected Information for which CE is required to account to an individual], BA and its agents or subcontractors shall make available to CE the information required to provide an accounting of disclosures to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.528, as determined by CE. BA agrees to implement a process that allows for an accounting to be collected and maintained by BA and its agents or subcontractors for at least six (6) years prior to the request. At a minimum, such information shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure. In the event that the request for an accounting is delivered directly to BA or its agents or subcontractors, BA shall within five (5) days of a request forward it to CE in writing. It shall be CE's responsibility to prepare and deliver any such accounting requested. BA shall not disclose any Protected Information except as set forth in Sections 2.b. of this Addendum [45 C.F.R. Sections 164.504(e)(2)(ii)(G) and 165.528]. The provisions of this subparagraph h shall survive the termination of this Agreement.*
- i. Governmental Access to Records.** *BA shall make its internal practices, books and records relating to the use and disclosure of Protected Information available to CE and to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for purposes of determining BA's compliance with the Privacy Rule [45 C.F.R. Section 164.504(e)(2)(ii)(H)]. BA shall provide to CE a copy of any Protected Information that BA provides to the Secretary concurrently with providing such Protected Information to the Secretary.*
- j. Minimum Necessary.** *BA (and its agents or subcontractors) shall request, use and disclose only the minimum amount of Protected Information necessary to accomplish the purpose of the request, use or disclosure [45 C.F.R. Section 164.514(d)(3)].*
- k. Data Ownership.** *BA acknowledges that BA has no ownership rights with respect to the Protected Information.*
- l. Business Associate's Insurance.** *(If there is an insurance provision in the Contract, consider whether it is adequate to address risks associated with BA's use and disclosure of Protected Information under the Addendum.)*
- m. Notification of Breach.** *During the term of the Contract, BA shall notify CE within twenty-four (24) hours of any suspected or actual breach of security, intrusion or unauthorized use or disclosure of PHI of which BA becomes aware and/or any actual or suspected use or disclo-*

sure of data in violation of any applicable federal or state laws or regulations. BA shall take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations. (This provision should be negotiated.)

- n. **Audits, Inspection and Enforcement.** Within ten (10) days of a written request by CE, BA and its agents or subcontractors shall allow CE to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of Protected Information pursuant to this Addendum for the purpose of determining whether BA has complied with this Addendum; provided, however, that (i) BA and CE shall mutually agree in advance upon the scope, timing and location of such an inspection, (ii) CE shall protect the confidentiality of all confidential and proprietary information of BA to which CE has access during the course of such inspection; and (iii) CE shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by BA. The fact that CE inspects, or fails to inspect, or has the right to inspect, BA's facilities, systems, books, records, agreements, policies and procedures does not relieve BA of its responsibility to comply with this Addendum, nor does CE's (i) failure to detect or (ii) detection, but failure to notify BA or require BA's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of CE's enforcement rights under the Contract or Addendum. BA shall notify CE within ten (10) days of learning that BA has become the subject of an audit, compliance review, or complaint investigation by the Office for Civil Rights (This provision should be negotiated.)

3. Termination

- a. **Material Breach.** A breach by BA of any provision of this Addendum, as determined by CE, shall constitute a material breach of the Contract and shall provide grounds for *immediate* termination of the Contract, any provision in the Contract to the contrary notwithstanding. [45 C.F.R. Section 164.504(e)(2)(iii)].
- b. **Judicial or Administrative Proceedings.** CE may terminate the Contract, effective immediately, if (i) BA is named as a defendant in a criminal proceeding for a violation of HIPAA, the HIPAA Regulations or other security or privacy laws or (ii) a finding or stipulation that the BA has violated any standard or requirement of HIPAA, the HIPAA Regulations or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.
- c. **Effect of Termination.** Upon termination of the Contract for any reason, BA shall, at the option of CE, return or destroy all Protected Information that BA or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If return or destruction is not feasible, as determined by CE, BA shall continue to extend the protections of Section 2 of this Addendum to such information, and limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible [45 C.F.R. Section 164.504(e)(ii)(2)(I)]. If CE elects destruction of the PHI, BA shall certify in writing to CE that such PHI has been destroyed.

4. **Indemnification**

[If there is an indemnification provision in the Contract, consider whether it is sufficient to address potential liabilities arising from breach of the terms of the Addendum.]

5. **Limitation of Liability**

[A covered entity may wish to seek an exception to any limitation of liability provision for the benefit of the business associate with regard to damages related to a breach of the business associate's privacy or security obligations under the Contract or Addendum.]

6. **Disclaimer**

CE makes no warranty or representation that compliance by BA with this Addendum, HIPAA or the HIPAA Regulations will be adequate or satisfactory for BA's own purposes. BA is solely responsible for all decisions made by BA regarding the safeguarding of PHI.

7. **Certification**

To the extent that CE determines that such examination is necessary to comply with CE's legal obligations pursuant to HIPAA relating to certification of its security practices, CE or its authorized agents or contractors, may, at CE's expense, examine BA's facilities, systems, procedures and records as may be necessary for such agents or contractors to certify to CE the extent to which BA's security safeguards comply with HIPAA, the HIPAA Regulations or this Addendum.

8. **Amendment**

- a. **Amendment to Comply with Law.** *The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of the Contract or Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the Privacy Rule, the Security Rule and other applicable laws relating to the security or confidentiality of PHI. The parties understand and agree that CE must receive satisfactory written assurance from BA that BA will adequately safeguard all Protected Information. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the Privacy Rule or other applicable laws. CE may terminate the Contract upon thirty (30) days written notice in the event (i) BA does not promptly enter into negotiations to amend the Contract or Addendum when requested by CE pursuant to this Section or (ii) BA does not enter into an amendment to the Contract or Addendum providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of applicable laws.*
- b. **Amendment of Attachment A.** *Attachment A may be modified or amended by mutual agreement of the parties at any time without amendment of the Contract or Addendum.*

9. Assistance in Litigation or Administrative Proceedings

BA shall make itself, and any subcontractors, employees or agents assisting BA in the performance of its obligations under the Contract or Addendum, available to CE, at no cost to CE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers or employees based upon a claimed violation of HIPAA, the Privacy Rule or other laws relating to security and privacy, except where BA or its subcontractor, employee or agent is a named adverse party.

10. No Third-Party Beneficiaries

Nothing express or implied in the Contract or Addendum is intended to confer, nor shall anything herein confer, upon any person other than CE, BA and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

11. Effect on Contract

Except as specifically required to implement the purposes of this Addendum, or to the extent inconsistent with this Addendum, all other terms of the Contract shall remain in force and effect.

12. Interpretation

The provisions of this Addendum shall prevail over any provisions in the Contract that may conflict or appear inconsistent with any provision in this Addendum. This Addendum and the Contract shall be interpreted as broadly as necessary to implement and comply with HIPAA and the Privacy Rule. The parties agree that any ambiguity in this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the Privacy Rule.

IN WITNESS WHEREOF, the parties hereto have duly executed this Addendum as of the Addendum Effective Date.

COVERED ENTITY

BUSINESS ASSOCIATE

By: _____
Print Name: _____
Title: _____
Date: _____

By: _____
Print Name: _____
Title: _____
Date: _____

BUSINESS ASSOCIATE ADDENDUM: ATTACHMENT A

If there are no additional terms, it is not necessary to use this Attachment. This Attachment may be executed after the parties have entered into the Addendum to reflect additional specifications relating to the use or disclosure of Protected Information.

This Attachment sets forth additional terms to the Addendum to the [FULL NAME OF CONTRACT] (“Contract”) by and between CE and BA, dated _____, and is effective as of _____ (the “Attachment Effective Date”). This Attachment may be amended from time to time as provided in Section 8.b. of the Addendum.

1. **Additional Permitted Uses.** In addition to those purposes set forth in Section 2.a. of the Addendum, BA may use Protected Information as follows: _____

2. **Additional Permitted Disclosures.** In addition to those purposes set forth in Section 2.b. of the Addendum, BA may disclose Protected Information as follows: _____

3. **Subcontractor(s).** The parties acknowledge that the following subcontractors or agents of BA shall receive Protected Information in the course of assisting BA in the performance of its obligations under the Contract and the Addendum: _____

4. **Receipt.** BA’s receipt of Protected Information pursuant to the Contract and Addendum shall be deemed to occur as follows, and BA’s obligations under the Addendum shall commence with respect to such PHI upon such receipt: _____

5. **Additional Restrictions on Use of Data.** CE is a Business Associate of certain other Covered Entities and, pursuant to such obligations of CE, BA shall comply with the following restrictions on the use and disclosure of Protected Information: _____

6. **Additional Terms.** *[This section may include specifications for disclosure format, method of transmission, use of an intermediary, use of digital signatures or PKI, authentication, additional security or privacy specifications, de-identification or re-identification of data and other additional terms.]* _____

COVERED ENTITY

BUSINESS ASSOCIATE

By: _____

Print Name: _____

Title: _____

Date: _____

By: _____

Print Name: _____

Title: _____

Date: _____