**APPENDIX PR 11-B**

# Business Associate Addendum

*This model contract language 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. The language of this addendum is intended to supplement an existing contract for services. Alternatively, the language of the addendum may be incorporated into the language of an existing contract, thereby creating one document. The parties to this agreement should not use any model agreement, including this one, without careful legal review and necessary modifications.*

*Optional provisions (that is, provisions not required by state or federal law) are indicated in italics.*

---

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"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), 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(a) and (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. **Breach** shall have the meaning given to such term under the HITECH Act and HIPAA Regulations [42 U.S.C. Section 17921 and 45 C.F.R. Section 164.402].

   b. **Breach Notification Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and D.

   c. **Business Associate** shall have the meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including, but not limited to, 42 U.S.C. Section 17938 and 45 C.F.R. Section 160.103.

d. **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.

e. ***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.*

f. **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.

g. **Electronic Protected Health Information** means Protected Health Information that is maintained in or transmitted by electronic media.

h. **Electronic Health Record** shall have the meaning given to such term in the HITECT Act, including, but not limited to, 42 U.S.C. Section 17921.

i. ***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.*

j. **Privacy Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.

k. **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, receives, maintains 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].

l. **Protected Information** shall mean PHI provided by CE to BA or created, maintained, received or transmitted by BA on CE's behalf.

m. **Security Incident** shall have the meaning given to such term under the Security Rule, including, but not limited to, 45 C.F.R. Section 164.304.

n. **Security Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

o. **Unsecured PHI** shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h) and 45 C.F.R. Section 164.402.

2. **Obligations of Business Associate**

a. **Permitted Uses.** BA shall use Protected Information only for the purpose of performing BA's obligations under the Contract and as permitted or required under the Contract and Addendum, or as required by law. Further, BA shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so used by CE. *However, BA may use Protected Information as necessary (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 relating to the Health Care Operations of CE* [45 C.F.R. Sections 164.504(e)(2) and 164.504(e)(4)(i)]. [List any other permitted uses here: _____.]

b. **Permitted Disclosures.** BA shall disclose Protected Information only for the purpose of performing BA's obligations under the Contract and as permitted or required under the Contract and Addendum, or as required by law. BA shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so disclosed by CE. *However, BA may disclose Protected Information as necessary (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 relating to 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 used or disclosed only 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, suspected breaches, security incidents, or unauthorized uses or disclosures of the Protected Information in accordance with paragraph 2. m. of the Addendum, to the extent it has obtained knowledge of such occurrences [42 U.S.C. Section 17932; 45 C.F.R. Section 164.504(e)]. [List any other permitted disclosures here: _ _____.]

c. **Prohibited Uses and Disclosures.** BA shall not use or disclose PHI other than as permitted or required by the Contract and Addendum, or as required by law. BA shall not use or disclose Protected Information for fundraising or marketing purposes. BA shall not disclose Protected Information to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates [42 U.S.C. Section 17935(a) and 45 C.F.R. Section 164.522(a)(vi)]. BA shall not directly or indirectly receive remuneration in exchange for Protected Information, except with the prior written consent of CE and as permitted by the HITECH Act, 42 U.S.C. Section 17935(d)(2), and the HIPAA regulations, 45 C.F.R. Section 164.502(a)(5)(ii); however, this prohibition shall not affect payment by CE to BA for services provided pursuant to the Contract. *[This provision will need to be modified if the underlying Contract is for fundraising or marketing purposes, or for a purpose for which the HITECH Act and HIPAA Regulations permits remuneration in exchange for PHI, such as a copy service providing copies of medical records to patients.]*

d. **Appropriate Safeguards.** BA shall implement appropriate safeguards to prevent the use or disclosure of Protected Information other than as permitted by the Contract or Addendum, including, but not limited to, administrative, physical and technical safeguards in accordance with the Security Rule, including, but not limited to, 45 C.F.R. Sections 164.308, 164.310, and 164.312. [45 C.F.R. Section 164.504(e)(2)(ii)(B); 45 C.F.R. Section 164.308(b)]. BA shall comply with the policies and procedures and documentation requirements of the Security Rule, including, but not limited to, 45 C.F.R. Section 164.316. [42 U.S.C. Section 17931]

e. **Business Associate's Subcontractors and Agents.** BA shall ensure that any agents and subcontractors that create, receive, maintain or transmit Protected Information on be-

half of BA, agree in writing to the same restrictions and conditions that apply to BA with respect to such Protected Information *[If the business associate creates, receives, maintains or transmits electronic PHI on behalf of the CE, the following language is required:]* and implement the safeguards required by paragraph 2. d. 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 five (5) days of a request by CE* to enable CE to fulfill its obligations under state law [Health and Safety Code Section 123110] and 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)]. If BA maintains Protected Information in electronic format, BA shall provide such information in electronic format as necessary to enable CE to fulfill its obligations under the HITECH Act and HIPAA Regulations, including, but not limited to, 42 U.S.C. Section 17935(e) and 45 C.F.R. Section 164.524.

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 a request by CE for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, BA and its agents and subcontractors shall make such Protected Information available to CE for amendment and incorporate any such amendment or other documentation to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.526. *If an 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 and of any approval or denial of amendment of Protected Information maintained by BA or its agents or subcontractors* [45 C.F.R. Section 164.504(e)(2)(ii)(F)].

h. **Accounting of Disclosures.** *[Within ten (10) days of a request by CE 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 and 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, and the HITECH Act, including but not limited to 42 U.S.C. Section 17935(c), 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 and subcontractors for at least six (6) years prior to the request. However, accounting of disclosures from an Electronic Health Record for treatment, payment or health care operations purposes are required to be collected and maintained for only three (3) years prior to the request, and only to the extent that BA maintains an Electronic Health Record. At a minimum, the information collected and maintained 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. *If a patient submits a request for an accounting directly to BA or its agents or subcontractors, BA shall within five (5) days of the request forward it to CE in writing.*

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 HIPAA [45 C.F.R. Section 164.504(e)(2)(ii)(I)]. *BA shall provide CE a copy of any Protected Information and other documents and records that BA provides to the Secretary concurrently with providing such Protected Information to the Secretary.*

j. **Minimum Necessary.** BA, its agents and subcontractors shall request, use and disclose only the minimum amount of Protected Information necessary to accomplish the purpose of the request, use or disclosure. [42 U.S.C. Section 17935(b); 45 C.F.R. Section 164.514(d)] BA understands and agrees that the definition of "minimum necessary" is in flux and shall keep itself informed of guidance issued by the Secretary with respect to what constitutes "minimum necessary."

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.)*

m. **Notification of Possible Breach.** BA shall notify CE *within twenty-four (24) hours* of any suspected or actual breach of Protected Information; any use or disclosure of Protected Information not permitted by the Contract or Addendum; any security incident (i.e., any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system) related to Protected Information, and any actual or suspected use or disclosure of data in violation of any applicable federal or state laws by BA or its agents or subcontractors. The notification shall include, to the extent possible, the identification of each individual whose unsecured Protected Information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed, as well as any other available information that CE is required to include in notification to the individual, the media, the Secretary, and any other entity under the Breach Notification Rule and any other applicable state or federal laws, including, but not limited, to 45 C.F.R. Section 164.404 through 45 C.F.R. Section 164.408, at the time of the notification required by this paragraph or promptly thereafter as information becomes available. BA shall take (i) prompt corrective action to cure any deficiencies and (ii) any action pertaining to unauthorized uses or disclosures required by applicable federal and state laws. (This provision should be negotiated.) [42 U.S.C. Section 17921; 45 C.F.R. Section 164.504(e)(2)(ii)(C); 45 C.F.R. Section 164.308(b)]

n. **Breach Pattern or Practice by Business Associate's Subcontractors and Agents.** Pursuant to 42 U.S.C. Section 17934(b) and 45 C.F.R. Section 164.504(e)(1)(ii), if the

BA knows of a pattern of activity or practice of a subcontractor or agent that constitutes a material breach or violation of the subcontractor or agent's obligations under the Contract or Addendum or other arrangement, the BA must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, the BA must terminate the Contract or other arrangement if feasible. *BA shall provide written notice to CE of any pattern of activity or practice of a subcontractor or agent that BA believes constitutes a material breach or violation of the subcontractor or agent's obligations under the Contract or Addendum or other arrangement within five (5) days of discovery and shall meet with CE to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.*

o. ***Audits, Inspection and Enforcement.*** *Within ten (10) days of a request by CE, BA and its agents and subcontractors shall allow CE or its agents or subcontractors 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 or maintains adequate security safeguards; 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 five (5) days of learning that BA has become the subject of an audit, compliance review, or complaint investigation by the Office for Civil Rights or other state or federal government entity.*

3. **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.]*

_____

_____

_____

4. **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 HITECH Act, 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 HITECH Act, 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 and its agents and 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 and satisfy the obligations of Section 2 of this Addendum to such information, and limit further use and disclosure of such PHI to those purposes that make the return or destruction of the information infeasible [45 C.F.R. Section 164.504(e)(ii)(2)(J)]. If CE elects destruction of the PHI, BA shall certify in writing to CE that such PHI has been destroyed in accordance with the Secretary's guidance regarding proper destruction of PHI.

5. ***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.]*

6. ***Limitation of Liability***

*[A covered entity may wish to seek an exception to any limitation of liability provision that benefits 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.]*

7. ***Disclaimer***

*CE makes no warranty or representation that compliance by BA with this Addendum, HIPAA, the HITECH Act, 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.*

8. ***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 HITECH Act, the HIPAA regulations and other applicable state or federal 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 HITECH Act, the HIPAA regulations 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.*

9. ***Litigation or Administrative Proceedings***

*BA shall notify CE within forty-eight (48) hours of any litigation or administrative proceedings commenced against BA or its agents or subcontractors. In addition, BA shall make itself, and any subcontractors, employees and 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 HITECH Act, the HIPAA regulations, or other state or federal 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, the HITECH Act, the HIPAA regulations, and other state and federal laws related to security and privacy. The parties agree that any ambiguity in this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act, the HIPAA regulations, and other state and federal laws related to security and privacy.*

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

| COVERED ENTITY | BUSINESS ASSOCIATE |
|---|---|
| By: _____ | By: _____ |
| Print Name: _____ | Print Name: _____ |
| Title: _____ | Title: _____ |
| Date: _____ | Date: _____ |