

HIPAA Business Associate Contract Sample Language

(revised to reflect the HIPAA Security Rule published on April 17, 2003)

<Customer>

and

<Vendor>

This Business Associate Addendum ("Addendum"), effective on the Compliance Date (defined in Section 5.3 below) is entered into by and between <Vendor>, and _____ with an address at _____, on behalf of itself and its subsidiaries listed on Schedule A attached hereto ("Customer") (each a "Party" and collectively the "Parties").

1. **BACKGROUND AND PURPOSE.** The Parties have entered into one or more contracts described or listed on Schedule B attached hereto (the "Underlying Contract(s)"), which require <Vendor> to be provided with, to have access to, and/or create Protected Health Information that is subject to the federal regulations issued pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") and codified at 45 C.F.R. parts 160 and 164 ("HIPAA Regulations"). This Addendum shall supplement and/or amend each of the Underlying Contract(s) only with respect to <Vendor>'s receipt, use and creation of PHI under the Underlying Contract(s) to allow Customer to comply with sections 164.502(e) and 164.314(a)(2)(i) of the HIPAA Regulations. Except as so supplemented and/or amended, the terms of the Underlying Contract(s) shall continue unchanged and shall apply with full force and effect to govern the matters addressed in this Addendum and in each of the Underlying Contract(s). [This provision can be adjusted/scaled using Schedule B]

2. **DEFINITIONS.** Unless otherwise defined in this Addendum, all capitalized terms used in this Addendum have the meanings ascribed in the HIPAA Regulations, provided, however, that "PHI" and "ePHI" shall mean Protected Health Information and Electronic Protected Health Information, respectively, as defined in 45 C.F.R. §160.103, limited to the information <Vendor> received from or created or received on behalf of Customer as Customer's Business Associate.

3. **OBLIGATIONS OF THE PARTIES WITH RESPECT TO PHI.**

3.1 **Obligations of <Vendor>.** With regard to its use and/or disclosure of PHI, <Vendor> agrees to:

- a. not use or disclose PHI other than as permitted or required by this Addendum or as required by law. [§164.504 (e)(2)(ii)(A)]
- b. use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Addendum. [§164.504 (e)(2)(ii)(B)]
- c. report to Customer any use or disclosure of PHI not provided for by this Addendum of which <Vendor> becomes aware. [§164.504 (e)(2)(ii)(C)]

AHA-NEMA HIPAA Business Associate Contract Sample Language
(Reflects the privacy and security rules)

- d. ensure that any agents and subcontractors to whom it provides PHI received from, or created or received by <Vendor> on behalf of Customer agree to the same restrictions and conditions set forth in the business associate provisions of the HIPAA Regulations that apply through this Addendum to <Vendor> with respect to such information. [§164.504 (e)(2)(ii)(D)]
- e. within twenty (20) days of receiving a written request from Customer, make available to the Customer PHI necessary for Customer to respond to individuals' requests for access to PHI about them in the event that the PHI in <Vendor>'s possession constitutes a Designated Record Set. [§164.504 (e)(2)(ii)(E)]
- f. within forty (40) days of receiving a written request from Customer, make available to the Customer PHI for amendment and incorporate any amendments to the PHI in accordance with 45 C.F.R. Part 164 Subpart E ("Privacy Rule") in the event that the PHI in <Vendor>'s possession constitutes a Designated Record Set. [§164.504 (e)(2)(ii)(F)]
- g. within forty (40) days of receiving a written request from Customer, make available to the Customer the information required for the Customer to provide an accounting of disclosures of PHI as required by the Privacy Rule. [§164.504 (e)(2)(ii)(G)]
- h. make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary of HHS for purposes of determining Customer's compliance with the Privacy Rule. [§164.504 (e)(2)(ii)(H)]
- i. upon the expiration or termination of an Underlying Contract, return to Customer or destroy all PHI, including such information in possession of <Vendor>'s subcontractors, as a result of the Underlying Contract at issue and retain no copies, if it is feasible to do so. If return or destruction is infeasible, <Vendor> agrees to extend all protections, limitations and restrictions contained in this Addendum to <Vendor>'s use and/or disclosure of any retained PHI, and to limit further uses and/or disclosures to the purposes that make the return or destruction of the PHI infeasible. This provision shall survive the termination or expiration of this Addendum and/or any Underlying Contract. [§164.504 (e)(2)(ii)(I)]
- j. use reasonable commercial efforts to mitigate any harmful effect that is known to <Vendor> of a use or disclosure of PHI by <Vendor> in violation of the requirements of this Addendum.
- k. implement administrative, physical, and technical safeguards ("Safeguards") that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI as required by 45 C.F.R. Part 164 Subpart C ("Security Rule") [§164.314 (a)(2)(i)(A)];
- l. ensure that any agent and subcontractor to whom <Vendor> provides ePHI agrees to implement reasonable and appropriate safeguards to protect ePHI [§164.314 (a)(2)(i)(B)];
- m. report promptly to Covered Entity any Security Incident of which <Vendor> becomes aware. [§164.314 (a)(2)(i)(C)]; and
- n. make its policies, procedures and documentation required by the Security Rule relating to the Safeguards available to the Secretary of HHS for purposes of determining Customer's compliance with the Security Rule. [68 Fed. Reg. 8334, 8359]

3.2 Permitted Uses and Disclosures of PHI. Except as otherwise specified in this Addendum, <Vendor> may make any and all uses and disclosures of PHI necessary to perform its obligations under the Underlying Contracts. Unless otherwise limited herein, <Vendor> may:

AHA-NEMA HIPAA Business Associate Contract Sample Language
(Reflects the privacy and security rules)

- a. use the PHI in its possession for its proper management and administration and to carry out the legal responsibilities of <Vendor> [§164.504 (e)(4)(i)];
- b. disclose the PHI in its possession to a third party for the purpose of <Vendor>'s proper management and administration or to carry out the legal responsibilities of <Vendor>, provided that the disclosures are required by law or <Vendor> obtains reasonable assurances from the third party regarding the confidential handling of such PHI as required under the Privacy Rule [§164.504 (e)(4)(ii)];
- c. provide Data Aggregation services relating to the health care operations of the Customer [§164.504 (e)(2)(i)(B)] and
- d. de-identify any and all PHI obtained by <Vendor> under this Addendum, and use such de-identified data, all in accordance with the de-identification requirements of the Privacy Rule. [§164.502 (d)(1)] [This provision should be adjusted to reflect the uses and disclosures required to perform the Underlying Contract(s).]

4. **TERMINATION BY CUSTOMER.** Should Customer become aware of a breach of a material term of this Addendum by <Vendor>, the Customer shall provide <Vendor> with written notice of such breach in sufficient detail to enable <Vendor> to understand the specific nature of the breach. Customer shall be entitled to terminate the Underlying Contract associated with such breach if, after Customer provides the notice to <Vendor>, <Vendor> fails to cure the breach within a reasonable time period specified by Customer in such notice; provided, however, that such time period specified by Customer shall be based on the nature of the breach involved. [§§164.504 (e)(1)(ii)(A),(B) & 164.314 (a)(2)(i)(D)]

5. **MISCELLANEOUS.**

- 5.1 Interpretation. The terms of this Addendum shall prevail in the case of any conflict with the terms of any Underlying Contract to the extent necessary to allow Customer to comply with the HIPAA Regulations. The bracketed citations to the HIPAA Regulations in several paragraphs of this Addendum are for reference only and shall not be relevant in interpreting any provision of this Addendum, except as set forth in Section 5.3 below.
- 5.2 No Third Party Beneficiaries. Nothing in this Addendum shall confer upon any person other than the Parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
- 5.3 Compliance Date. For the purposes of this Addendum, the Compliance Date for a section of this Addendum is defined as the date on which the HIPAA Regulations require compliance by the Customer with the referenced provision of the HIPAA Regulations; if multiple regulations are referenced, the one requiring earliest compliance shall apply. If a section does not reference a provision of the HIPAA Regulations, for each Underlying Contract such section shall be effective on the later of April 14, 2003 or the effective date of such Underlying Contract.
- 5.4 Amendment. To the extent that any relevant provision of the HIPAA Regulations is materially amended in a manner that changes the obligations of Business Associates or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s) to this Addendum to give effect to these revised obligations.

AHA-NEMA HIPAA Business Associate Contract Sample Language
(Reflects the privacy and security rules)

IN WITNESS WHEREOF, each of the undersigned has caused this Addendum to be duly executed in its name and on its behalf.

CUSTOMER

<Vendor>

By: _____

By: _____

Print Name: _____

Print Name: _____

Print Title: _____

Print Title: _____

SCHEDULE A
CUSTOMER

Customer Parent:

Customer Subsidiaries Covered By this Addendum:

SCHEDULE B
UNDERLYING CONTRACTS

[Describe the scope of contracts covered by this Agreement using 1 of the following 2 options:

1. This Schedule may be used to generally describe the scope of contracts between the Parties using the following language: "The Parties have entered into, and may in the future enter into, one or more agreements, written or oral, that require <Vendor> to be provided with, to have access to, and/or to create Protected Health Information."

OR

2. List the specific contracts covered by this Agreement (Contract Title, Customer Name, Date and Contract Number).]