

# HIPAA OMNIBUS RULE BUSINESS ASSOCIATES AGREEMENT

under OMNIBUS RULE

## “A Business Vendor Confidentiality Agreement”

This document is required to be signed by the Business Associate and maintained on file by Covered Entity to comply with Omnibus Rule of 2013, and Effective March 26, 2013. Signatures need to be made by:

**September 23, 2013** for new Business Associates Agreements, or, if after this date, at inception of the business date.

**September 22, 2014** for Business Associate Agreements currently on-file. This new version needs to be signed and kept on-file.

**BUSINESS ASSOCIATES ARE URGED TO GET AND USE THEIR OWN SUB CONTRACTORS AGREEMENTS. WE URGE YOU TO NOT GET INVOLVED IN THAT PROCESS OR YOU MAY BECOME LIABLE FOR ANY NON COMPLIANT ACTIVITIES.**

### Term

The Term of this Agreement shall be effective as of \_\_\_\_\_ (**Today's Date**), and shall terminate upon the date that Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

### Definitions

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Healthcare Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

#### Specific definitions:

**(a) Business Associate.** “*Business Associate*” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean \_\_\_\_\_  
\_\_\_\_\_ (**Name of Vendor / Business Associate**).

**(b) Covered Entity.** “*Covered Entity*” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean \_\_\_\_\_  
\_\_\_\_\_ (**Name of Your Healthcare Facility / Covered Entity**).

**(c) HIPAA Rules.** “*HIPAA Rules*” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

## Obligations and Activities of Business Associate

(Business Vendor) agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to ePHI electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to Covered Entity any use or disclosure of PHI protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware; The Business Associate, *will report these immediately or not more than 5 business days after such a discovery.*

The Business Associate *will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the Covered Entity as its own breach.* Reporting is made to: HHS at this link:

<http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html>

*(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)*

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any Subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;

(e) Make available PHI (protected health information) in a designated record set to the “Covered Entity” as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.524;

The Business Associate will respond to a request for access that the Business Associate receives directly from an individual for responsive business purpose, this will be either ***via email, (read-receipt option) and /or via registered mail, within 5 business days of a request.***

(f) The Business Associate will make any amendment(s) to PHI protected health information in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.526; and:

The Business Associate will respond to a ***request for amendment*** when received directly from the individual either ***via email, (read-receipt option) and /or via registered mail, within 5 days*** of a request and the Business Associate will forward the individual’s request to the Covered Entity ***with any amendments*** to the information in the designated record set will be incorporated.

(g) Maintain and make available the information required to provide an ***accounting of disclosures*** to the Covered Entity and also to the Individual, as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.528;

The Business Associate will respond to a request for accounting of disclosures when received directly from the individual either **via email, (read-receipt option) and /or via registered mail, either, within 5 days** of a request **and** the Business Associate will **forward the individual's request to the Covered Entity** with any **Accounting of Disclosures** to the information in the designated record set will be incorporated.

**(h)** To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and

**(i)** The Business Associate will make its internal practices, books, and records available to legal inspectors, The HHS and Covered Entity for purposes of determining compliance with the HIPAA Rules.

### **Permitted Uses and Disclosures by Business Associate**

**(a)** Business Associate may only use or disclose PHI protected health information pertaining only to situations that deem it necessary to perform the services set forth in the Business Associates & Covered Entities governing Service Agreement/ Contract.

In addition to other permissible purposes, the Business Associate is authorized to use PHI protected health information to **de-identify the information** in accordance with 45 CFR 164.514(a)-(c). The Business Associate may de-identify the information, permitted uses and disclosures by means legal and necessary to formulate this identity.

**(b)** Business Associate may use or disclose PHI protected health information as required by law.

**(c)** Business Associate agrees to make uses and disclosures and requests for PHI protected health information in timely and legal fashion consistent with Covered Entity's minimum necessary policies and procedures, which are defined as: the *least* effort and information disclosure necessary to complete this task.

**(d)** Business Associate may not use or disclose PHI protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity except for the specific uses and disclosures set forth below:

**(e)** Business Associate may use PHI protected health information for the proper management and administration to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law and that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed. Notifications will be made to the Business Associate of any instances in which the confidentiality of the PHI information has been breached.

**(f)** Business Associate may provide data aggregation services relating to the healthcare operations of the Covered Entity.

### **Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions**

**(a)** Covered Entity may notify Business Associate of any limitation(s) in the Notice of Privacy Practices of Covered

Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI protected health information.

**(b)** Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI protected health information, to the extent that such changes may affect Business Associate's use or disclosure of PHI protected health information.

**(c)** Covered Entity shall notify Business Associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI protected health information.

### **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 Subpart E of 45 CFR Part 164 if done by Covered Entity. The exception would be if the Business Associate will use or disclose PHI protected health information for, data aggregation or management and administration and legal responsibilities of the Business Associate.

### **Termination**

**(a) Termination for Cause.** Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the Agreement (and Business Associate has not cured the breach or ended the violation within the time specified by Covered Entity).

### **(b) Obligations of Business Associate Upon Termination.**

Business Associate shall retain no copies of the protected health information except to use or disclose PHI protected health information for its own management and administration or to carry out its legal responsibilities and the Business Associate needs to retain PHI protected health information for such purposes after termination of the agreement.

Upon termination of this Agreement for any reason, Business Associate, with respect to PHI protected health information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

1. Retain only that PHI protected health information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to covered entity or destroy the remaining PHI protected health information that the Business Associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to ePHI electronic protected health information to prevent use or disclosure of the PHI protected health information, other than as provided for in this Section, for as long as Business Associate retains the PHI protected health information;
4. Not use or disclose the PHI protected health information retained by Business Associate other than for the

purposes for which such PHI protected health information was retained and subject to the same conditions set in the Permitted Uses and Disclosures by Business Associate sections (e) and (f) of this document, applied prior to termination; and

5. Return to Covered Entity or destroy the PHI protected health information retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

The Business Associate may be asked by the Covered Entity to transmit the PHI protected health information to another Business Associate of the Covered Entity at termination. The Business Associate would comply, confirm the transfer and then ensure the destruction of PHI protected health information created, received, or maintained by subcontractors.

**(c) Survival.** The obligations of Business Associate under this Section shall survive the termination of this Agreement.

#### **Miscellaneous [Optional]**

**(a) Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law or law changes.

**(b) Interpretation.** Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules by the Business Associates legal counsel.

**This document was replicated from** The Omnibus Rule model form is available at: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>.

**BUSINESS ASSOCIATES ADDENDUM  
SIGNATURE PAGE—(RETAIN ON FILE)**

THIS SIGNATURE PAGE—ADDENDUM (hereafter “Addendum”) is entered into this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_, by and between \_\_\_\_\_ (hereafter “Business Associate”) and \_\_\_\_\_ (hereafter “Healthcare Facility”), for themselves and their respective successors and assigns.

WHEREAS, the parties hereto desire to modify the aforementioned Agreement to set forth the terms and conditions under which information created or received by Business Associate on behalf of this Healthcare Facility (hereafter collectively referred to as protected health information or “PHI”) may be used or disclosed under the Health Insurance Portability and Accountability Act “Omnibus Rule” of 2013 and regulations enacted thereunder (hereafter “HIPAA”);

THEREFORE, both parties, for valuable consideration from each party to the other, the receipt and sufficiency of which is hereby acknowledged, do hereby mutually agree that the Agreement shall continue in full force and effect with the following modifications and additions, to wit: (additions or modifications state below, must comply with HIPAA Omnibus Rules):

---

---

---

---

---

---

---

---

1. Except as amended by this Addendum, all terms, conditions and covenants of the Agreement are valid, shall remain in full force and effect, and hereby are ratified and confirmed.
2. Any inconsistencies between this Addendum and the Agreement shall be governed by this Addendum.
3. A copy of this Addendum shall be as effective as the original.

IN WITNESS WHEREOF, the parties hereto have entered into this Agreement as of the date first written above.

**Name of Practice (Covered Entity)**

**Name of Business Associate (Vendor)**

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Print name and title

\_\_\_\_\_  
Print name and title