

## BUSINESS ASSOCIATE ADDENDUM

**[To be used whenever Covered Entity already has a written contract with a business associate; this addendum incorporates HIPAA's Privacy Rule and Security Rule requirements into the existing agreement]**

This HIPAA Addendum ("Addendum") is entered into this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_, by and between \_\_\_\_\_ ("Business Associate") and \_\_\_\_\_ ("Covered Entity") and amends the \_\_\_\_\_ Agreement ("Agreement") previously entered into between Business Associate and Covered Entity.

Covered Entity is a health care provider. Pursuant to federal laws and regulations, including the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Covered Entity has an obligation to protect certain health information of its customers ("Protected Health Information"). As part of this obligation, Covered Entity must receive assurances from any business associate who receives or has access to Covered Entity's Protected Health Information that the business associate will protect the information in the same way as Covered Entity.

In performing services for Covered Entity, Business Associate may receive, access or create Protected Health Information on behalf of Covered Entity.

In consideration for Business Associate's access to and/or use of Protected Health Information for those purposes allowed by HIPAA and consistent with the terms of the Agreement, Business Associate and Covered Entity agree as follows:

**1. Definitions.** As used in this Addendum:

1.1. "Breach Notification Standards" shall mean the HIPAA regulations governing notification in the case of breach of unsecured Protected Health Information as set forth at 45 CFR § Part 164, Subpart D, as they exist now or as they may be amended.

1.2. "Designated Record Set" shall mean a group of records maintained by or for Covered Entity that is (i) the medical records and billing records about individuals maintained by or for Covered Entity, (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for Covered Entity to make decisions about individuals. As used herein, the term "Record" means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for Covered Entity.

1.3. "HIPAA" shall mean the Health Insurance Portability and Accountability Act, Public Law 104-91, and any amendments thereto.

1.4. "HIPAA Transaction" shall mean Transactions as defined in 45 CFR § 160.103 of the Transaction Standards.

1.5. “HITECH Act” means the Health Information Technology for Economic and Clinical Health Act, found in the American Recovery and Reinvestment Act of 2009 at Division A, title XIII and Division B, Title IV.

1.6. “Individual” shall have the same meaning as the term “individual” in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

1.7. “Minimum Necessary” shall have the meaning set forth in 45 CFR § 164.502(b).

1.8. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR § Part 160 and Part 164, as they exist now or as they may be amended.

1.9. “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR § 160.103, limited to the information that Business Associate accesses, creates, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses on behalf of Covered Entity.

1.10. “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR § 164.103.

1.11. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.

1.12. “Security Standards” shall mean the Security Standards, 45 CFR § Part 160 and Part 164, Subsection C as they exist now or as they may be amended.

1.13. “Transaction Standards” shall mean the Standards for Electronic Transactions, 45 CFR § part 160 and part 162, as they exist now or as they may be amended.

1.14. Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in 45 CFR §§ 160.103, 164.103, 164.304, and 164.501.

## **2. Obligations and Activities of Business Associate.**

2.1. Business Associate agrees that it shall not, and that its directors, officers, employees, contractors and agents shall not, use or further disclose Protected Health Information other than as permitted or required by this Addendum or as Required By Law.

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

2.3. 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 Addendum.

2.4. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Addendum of which it becomes aware, or of any act or omission that violates the terms of this Addendum.

2.5. 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 in writing to the terms of a business associate agreement containing the same restrictions and conditions that apply through this Addendum to Business Associate with respect to such information.

2.6. Business Associate agrees to provide access, within ten (10) days of receipt of such request to Protected Health Information in a Designated Record Set, to Covered Entity or, if requested 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.]*

2.7. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual within ten (10) days of receipt of such request. If Business Associate provides Designated Record Sets to third parties, Business Associate shall ensure such records are also amended. *[Not necessary if business associate does not have protected health information in a designated record set.]*

2.8. Business Associate agrees to make its 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 Covered Entity, or at the request of Covered Entity to the Secretary, in a time and manner designated by Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

2.9. Business Associate agrees to document 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 and any additional regulations promulgated by the Secretary pursuant to HITECH Act § 13405(c). Business Associate agrees to implement an appropriate record keeping process that will track, at a minimum, the following information: (i) the date of the disclosure; (ii) the name of the entity or person who received the Protected Health Information, and if known, the address of such entity or person; (iii) a brief description of the Protected Health Information disclosed; and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure.

2.10. Within twenty (20) days of receipt of such request Business Associate agrees to provide to Covered Entity or to an Individual, information collected in accordance with Section 2.9 of this Addendum, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information during the six (6) years prior to the date on which the accounting was requested, in accordance with 45 CFR § 164.528.

2.11. In the event Business Associate receives a subpoena, court or administrative order or other discovery request or mandate for release of Protected Health Information, Business Associate will respond as permitted by 45 CFR § 164.512(e) and (f). Business Associate shall notify Covered Entity of the request as soon as reasonably practicable, but in any event within two (2) business days of receipt of such request.

2.12. Business Associate will not make any communications in violation of the restrictions on marketing in 45 CFR § 164.508(a)(3).

2.13. If Business Associate will communicate with any individuals who are the subject of Protected Health Information originating from or prepared for Covered Entity, Business Associate agrees to implement procedures to give timely effect to an individual's request to receive communications of Protected Health Information by alternative means or at alternative locations, pursuant to 45 CFR § 164.522(b), so as to ensure that Protected Health Information will only be communicated to those individuals designated in such a request as authorized to receive the Protected Health Information. If Business Associate provides records to agents, including subcontractors, who may also communicate with the individual, Business Associate shall ensure that the individual's request for communications by alternative means is provided to and given timely effect by such agents.

2.14. Business Associate shall not directly or indirectly receive or provide remuneration in exchange for any Protected Health Information in violation of 45 CFR § 164.508(a)(4).

2.15. Upon request from Health Plan Sponsor, Business Associate shall permit Health Plan Sponsor to review and audit Business Associate's policies, procedures and practices relating to the use and protection of Protected Health Information, including the right to audit contracts and relationships with agents and subcontractors who have access to Protected Health Information, and upon request shall provide Covered Entity with copies of relevant documents.

2.16. Electronic Transactions. Business Associate hereby represents and warrants that, to the extent that it is electronically transmitting any of the HIPAA Transactions for Covered Entity, the format and structure of such transmissions shall be in compliance with the Transaction Standards.

2.17. Electronic Data Security. To the extent that Business Associate creates, receives, maintains or transmits electronic Protected Health Information, Business Associate hereby represents and warrants that it:

2.17.1. Has implemented and documented administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic Protected Health Information that Business Associate creates, receives, maintains or transmits on behalf of Health Plan Sponsor consistent with the requirements of the HIPAA Security Standards;

2.17.2. Will ensure that any agent, including a subcontractor, to whom Business Associate provides electronic Protected Health Information agrees to sign a business associate agreement and implements reasonable and appropriate safeguards to protect the Protected Health Information; and

2.17.3. Will keep records of all security incidents involving Protected Health Information of which Business Associate becomes aware, and will report to Covered Entity all significant security incidents of which Business Associate becomes aware.

2.18. Breach Notification. Business Associate warrants that it has in place policies and procedures that are designed to detect inappropriate acquisition, access, use or disclosure of Protected Health Information and that it adequately trains its work force and agents on these procedures. Business Associate will notify Covered Entity within three (3) business days of discovering an acquisition, access, use or disclosure of Protected Health Information in a manner or for a purpose not permitted by the HIPAA Privacy Rule and within 30 calendar days of discovery will provide Covered Entity with the identification of each individual whose Protected Health Information has been or is reasonably believed by Business Associate to have been acquired, accessed, used or disclosed during such incident. Business Associate will assist Covered Entity in assessing whether the impermissible acquisition, access, use or disclosure of Protected Health Information compromises the security or privacy of such Protected Health Information. If Covered Entity determines that individuals whose data is affected by the impermissible acquisition, access, use or disclosure must be notified pursuant to the HIPAA Breach Notification Standards or other applicable law, Business Associate will reimburse Covered Entity's reasonable notification costs, including legal fees and other costs associate with determining its notification duty, drafting its notification letter, mailing the notification letter and staffing its call center.

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

3.1. General Use. Except as otherwise limited in this Addendum, 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 the Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity. In performing such services, Business Associate will comply with all Privacy Rule requirements that would apply to Covered Entity if Covered Entity were performing such services.

#### **3.2. Specific Use and Disclosure Provisions**

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

3.2.2. Except as otherwise limited in this Addendum, Business Associate may disclose Protected Health Information for the proper management and administration of 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 Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3.2.3. Except as otherwise limited in this Addendum, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).

#### **4. Obligations of Covered Entity.**

4.1. Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitations may affect Business Associate's use or disclosure of Protected Health Information. Business Associate will give timely effect to such limitations.

4.2. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information. Business Associate will give timely effect to such changes or revocations.

4.3. 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, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information. Business Associate will give timely effect to such restrictions.

4.4. 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, except as specifically allowed by section 3.2 of this Addendum.

#### **5. Term and Termination.**

5.1. Term. This Addendum shall be effective as of the date it is executed, 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.

5.2. Termination for Breach by Business Associate. Upon Covered Entity's knowledge of a material breach of the terms of this Addendum by Business Associate, Covered Entity shall either:

5.2.1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Agreement and this Addendum if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

5.2.2. Immediately terminate the Agreement and this Addendum if Business Associate has breached a material term of this Addendum and cure is not possible.

5.3. Other Conditions Allowing for Immediate Termination. Notwithstanding anything to the contrary in the Agreement or this Addendum, Covered Entity may terminate the

Agreement and this Addendum immediately upon written notice to Business Associate, without any term of notice and/or judicial intervention being required, and without liability for such termination, in the event that:

5.3.1. Business Associate (i) receives a Criminal Conviction, (ii) is excluded, barred or otherwise ineligible to participate in any government health care program, including but not limited to Medicare, Medicaid or Tricare; (iii) is named as a defendant in a criminal proceeding for a violation of any information privacy and protection law; or (iv) is found to have or stipulates that it has violated any privacy, security or confidentiality protection requirements under any applicable information privacy and protection law in any administrative or civil proceeding in which Business Associate has been joined.;

5.3.2. A trustee or receiver is appointed for any or all property of Business Associate;

5.3.3. Business Associate becomes insolvent or unable to pay debts as they mature, or ceases to so pay, or makes an assignment for benefit of creditors;

5.3.4. Bankruptcy or insolvency proceedings under bankruptcy or insolvency code or similar law, whether voluntary or involuntary, are properly commenced by or against Business Associate;

5.3.5. Business Associate is dissolved or liquidated.

5.4. Effect of Termination.

5.4.1. Except as provided in paragraph 5.4.2 of this section, upon termination of the Agreement or this Addendum, 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.

5.4.2. In the event that return or destruction of the Protected Health Information is infeasible, Business Associate shall extend the protections of this Addendum 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.

**6. Miscellaneous.**

6.1. Amendment. No provision of this Addendum may be modified except by a written document signed by a duly authorized representative of the parties. The parties agree to amend either the Agreement or this Addendum, as appropriate, to conform with any new or revised legislation, rules and regulations to which Covered Entity is subject now or in the future including, without limitation, the Privacy Rule, Security Standards or Transactions Standards

(collectively "Laws"). If within ninety (90) days of either party first providing written notice to the other of the need to amend the Agreement or Addendum to comply with Laws, the parties, acting in good faith, are i) unable to mutually agree upon and make amendments or alterations to the Agreement or Addendum to meet the requirements in question, or ii) alternatively, the parties determine in good faith that amendments or alterations to the requirements are not feasible, then either party may terminate the Agreement upon thirty (30) days written notice.

6.2. Assignment. No party may assign or transfer any or all of its rights and/or obligations under this Addendum or any part of it, nor any benefit or interest in or under it, to any third party without the prior written consent of the other party, which shall not be reasonably withheld.

6.3. Survival. The respective rights and obligations of Business Associate under section 5.4 of this Addendum shall survive the termination of this Addendum.

6.4. Interpretation. Any ambiguity in this Addendum shall be resolved to permit Covered Entity to comply with the Breach Notification Standards, Privacy Rule, Security Standards, and Transaction Standards. If there is an inconsistency between the language in the Agreement and this Addendum, the language in this Addendum shall control.

6.5. Right to Cure. In addition to any other rights Covered Entity may have in the Agreement, this Addendum, or by operation of law or in equity, if Covered Entity determines that Business Associate has violated a material term of this Addendum, Covered Entity may, at its option, cure or end any such violation. Covered Entity's cure of a breach of this Addendum shall not be construed as a waiver of any other rights Covered Entity has in the Agreement, this Addendum or by operation of law or in equity.

6.6. Indemnification. Business Associate shall indemnify and hold harmless Covered Entity for any and all claims, inquiries, costs or damages, including but not limited to any monetary penalties, that Covered Entity incurs arising from a violation by Business Associate of its obligations hereunder.

6.7. Exclusion from Limitation of Liability. To the extent that Business Associate has limited its liability under the terms of the Agreement, whether with a maximum recovery for direct damages or a disclaimer against any consequential, indirect or punitive damages, or other such limitations, all limitations shall exclude all damages to Covered Entity arising from Business Associate's breach of its obligations relating to the use and disclosure of Protected Health Information.

6.8. Third Party Rights. The terms of this Addendum are not intended, nor should they be construed, to grant any rights to any parties other than Business Associate and Covered Entity.

6.9. Minimum Necessary. Business Associate hereby represents and warrants that, for all Protected Health Information that Business Associate accesses or requests from Covered Entity for the purposes of providing services under the Agreement, it shall access or request only that amount of information that is minimally necessary to perform such services. In addition, for all uses and disclosures of Protected Health Information by Business Associate, Business



Associate represents and warrants that it shall institute and implement policies and practices to limit such uses and disclosures to that which is minimally necessary to perform its services under the Agreement. Business Associate shall determine the amount minimally necessary consistent with the requirements in 45 CFR § 164.502(b).

6.10. Compliance. Business Associate may use and disclose Protected Health Information only if such use or disclosure, respectively, is in compliance with each applicable requirement of 45 CFR 164 Subpart E, as required under 45 CFR § 164.500(c) and 45 CFR § 164.504(e)(2)(ii)(H) and this Addendum.

6.11. Injunctive Relief. Business Associate acknowledges and stipulates that its unauthorized use or disclosure of Protected Health Information while performing services pursuant to the Agreement or this Addendum would cause irreparable harm to Covered Entity, and in such event, Covered Entity shall be entitled, if it so elects, to institute and prosecute proceedings in any court of competent jurisdiction, either in law or in equity, to obtain damages and injunctive relief, together with the right to recover from Business Associate costs, including reasonable attorneys' fees, for any such breach of the terms and conditions of the Agreement or this Addendum.

6.12. Notice. All notices required under this Addendum shall be in writing and shall be deemed to have been given on the next day by fax or other electronic means or upon personal delivery, or in ten (10) days upon delivery in the mail, first class, with postage prepaid. Notices shall be sent to the addressees indicated below unless written notification of change of address shall have been given.

If to Covered Entity:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Tel: \_\_\_\_\_

Fax: \_\_\_\_\_

If to Business Associate:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Tel: \_\_\_\_\_

Fax: \_\_\_\_\_

6.13. Owner of Protected Health Information. Under no circumstances shall Business Associate be deemed in any respect to be the owner of any Protected Health Information used or disclosed by or to Business Associate pursuant to the terms of the Agreement or this Addendum.

**IN WITNESS WHEREOF**, the parties have executed this Addendum the day and year first written above.

**BUSINESS ASSOCIATE:**

\_\_\_\_\_  
Signed

\_\_\_\_\_  
Printed

\_\_\_\_\_  
Date

**COVERED ENTITY:**

\_\_\_\_\_  
Signed

\_\_\_\_\_  
Printed

\_\_\_\_\_  
Date

9092431