

## **BUSINESS ASSOCIATE ADDENDUM**

This Business Associate Addendum ("Addendum") may impose additional terms and conditions on the "Principal Agreement" (as defined in Section 1.2 below) by and between Covenant Medical Center, Inc. ("Covered Entity") and \_\_\_\_\_ ("Business Associate") (each a "Party" and collectively the "Parties"), and is effective as of the BAA Effective Date.

### **1. Interpretation and Scope**

#### **1.1 Definitions**

(a) The "BAA Effective Date" is the latter of the effective date of the Principal Agreement, or September 23, 2009.

(b) "Government Officials" include the Secretary and other government agencies with jurisdiction to issue and enforce PSR Rules, and includes their respective employees, contractors, and other agents.

(c) "Individual" has the same meaning as the term "individual" in 45 CFR § 160.103 and includes any person who qualifies as a personal representative under 45 CFR § 164.502(g).

(d) "Protected Health Information" or "PHI" has the same meaning as the term "protected health information" in 45 CFR § 160.103.

(e) The "Privacy and Security Rules" or "PSRs" include: the Health Insurance Portability and Accountability Act of 1996 and privacy and security regulations promulgated thereunder and codified at 45 C.F.R. parts 160 and 164; as well as administrative simplification regulations codified at 45 C.F.R. part 162 (collectively "HIPAA"); and the Health Information Technology for Economic and Clinical Health Act of 2009, including without limitation security breach notification requirements issued by the Secretary at 74 Fed. Reg. 42740-42770 (Aug. 24, 2009) ("HITECH").

(f) "Prompt" or "promptly" means within fifteen (15) days after a Party knows or, by exercising reasonable diligence should have known, of an event.

(g) A Party's "Related Parties" include the Party's directors/trustees, officers, employees, agents, contractors, affiliates, workforce members, and other representatives (exclusive of the other Party).

(h) "Required By Law" has the same meaning as the term "required by law" in 45 CFR § 164.103.

(i) "Secretary" refers to the Secretary of the Department of Health and Human Services or his or her designee.

All other terms defined the PSRs but not otherwise defined in this Addendum are used with the same meaning given to them in the PSRs.

1.2 Modification of Principal Agreement. The Parties have entered or plan to enter one or more agreements, which are listed on Schedule A as may be

amended from time to time (collectively the "Principal Agreement"). Covered Entity is or may be a "covered entity" within the meaning of the PSRs. Business Associate provides services or performs functions or activities for or on behalf of Covered Entity and in that capacity uses or discloses PHI; and, accordingly, is or may be a business associate to Covered Entity. This Addendum modifies the Principal Agreement only if, and to the extent that, Covered Entity is a "covered entity" and Business Associate is a "business associate" as those terms are defined at 45 CFR § 160.103

1.3 Current and Ongoing Compliance. This Addendum is intended and shall be construed to assure the Parties' respective compliance with the PSRs. Accordingly, any reference in this Addendum to a provision of the PSRs means the PSRs as in effect or as amended by law, regulation, or other agency directive; any addition to this Addendum mandated by the PSRs after the BAA Effective Date shall be deemed incorporated herein by reference; and any ambiguity in this Addendum shall be resolved to permit both Parties to comply with the PSRs.

1.4 HITECH Compliance Deadlines. Individual terms in this Addendum that are required to comply with HITECH but not HIPAA are effective as of the latter of the BAA Effective Date or the relevant HITECH compliance date.

1.5 Administrative Simplification. Under no circumstances shall any provision of the Principal Agreement or this Addendum be interpreted to permit Business Associate, in providing items or services to Covered Entity, to: (i) change the definition, data condition, or use of a data element or segment in a standard; (ii) add any data elements or segments to the maximum defined data set; (iii) use any code or data elements that are either marked "not used" in the standard's implementation specifications or are not in the standard's implementation specifications; or (iv) change the meaning or intent of the standard's implementation specifications.

## **2. Business Associate Obligations**

Business Associate shall, in providing items or services pursuant to the Principal Agreement, appropriately safeguard all PHI that Business Associate accesses, maintains, retains, modifies, records, stores, or otherwise holds, uses, or discloses (collectively "uses or discloses"). In particular, Business Associate shall:

2.1 Use or disclose PHI only if and to the extent required to perform functions or activities for or on behalf of Covered Entity under the Principal Agreement, permitted pursuant to Section 3 below, or Required By Law. In all cases, Business Associate's use and disclosure shall comply with applicable provisions of the PSRs, including without limitation HITECH's minimum necessary requirements, mandate to agree to certain requested restrictions on disclosure, and imposition of restrictions on marketing and fundraising activities in addition to those described in HIPAA.

2.2 Ensure that any subcontractor or other third party (other than a Government Official) to whom it provides PHI agrees in writing to the same restrictions and conditions that apply to Business Associate with respect to such information, including without limitation implementation of reasonable and appropriate safeguards to protect it. Business Associate shall retain such writing for no fewer than six (6) years, or such longer time as may be required by applicable

state law, after the conclusion of Business Associate's relationship with such third party.

2.3 Implement and use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Addendum. Such safeguards shall include, without limitation, administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI and electronic PHI ("ePHI") that Business Associate creates, receives, maintains, or transmits on behalf of the Covered Entity as required by the PSRs. Business Associate expressly agrees to comply with 45 CFR §§ 164.308, 164.310, 164.312, and 164.316 in connection with the creation, receipt, maintenance, or transmission of electronic PHI ("ePHI") for or on behalf of Covered Entity.

2.4 Business Associate acknowledges that Covered Entity is or may be a "creditor" with "covered accounts" under the "Red Flag Rules" issued by the Federal Trade Commission ("FTC"), under the Fair and Accurate Credit Transactions Act of 2003 at 16 CFR part 681. Business Associate represents and warrants that it has implemented policies and procedures consistent with FTC recommendations to detect Red Flags as defined by FTC, and shall promptly report any such identified Red Flags to Covered Entity and, as appropriate, to appropriate law enforcement officials.

2.5 Promptly report to the Covered Entity any use or disclosure of PHI not provided for by this Addendum, and any security incident (as defined at 45 CFR § 164.304) of which Business Associate becomes aware; provided, however, that any security incidents that are not breaches of unsecured PHI (as defined at 45 CFR § 164.402) and that do not, to the best of Business Associate's knowledge, information, and belief, result in any use or disclosure of ePHI in violation of this Addendum, may be reported in aggregate on at least a quarterly basis. In the event of a breach of unsecured PHI, Business Associate shall notify Covered Entity promptly without unreasonable delay, and in any event within sixty (60) days, of its discovery of such breach, the identification of each Individual whose unsecured PHI was or is reasonably believed to have been accessed, acquired, or disclosed during such breach. Business Associate shall fully cooperate with Covered Entity's review, investigation, and response to any such alleged security incident or breach.

2.6 Mitigate, to the extent practicable, any harmful effect that results from any use or disclosure of PHI by Business Associate or one of Business Associate's Related Parties in violation of the Principal Agreement or this Addendum.

2.7 If and to the extent Business Associate uses or discloses PHI in a Designated Record Set: promptly after receiving a request from Covered Entity or, as applicable, an Individual: (i) provide access to PHI in a Designated Record Set to Covered Entity or, as directed by the Covered Entity, to the Individual in order to meet the requirements of 45 CFR § 164.524, in such form and manner as may be required by the PSRs; and (ii) make any amendments or corrections to PHI in a Designated Record Set as directed or agreed by Covered Entity pursuant to 45 CFR § 164.526.

2.8 Maintain any records of disclosures of PHI as may be necessary to respond, or to enable Covered Entity to respond, to a request by an Individual for an accounting of disclosures in accordance with the PSRs. Business Associate shall provide such documentation to Covered Entity promptly upon request.

2.9 Make available to the Covered Entity and Government Officials Business Associate's internal practices, books and records relating to the use or disclosure of PHI and to the security of PHI received from, or created or received by the Business Associate for or on behalf of the Covered Entity, so that the Government Officials may evaluate the Parties' compliance with the PSRs.

2.10 Not directly or indirectly receive remuneration in exchange for an Individual's PHI except as specifically authorized by Covered Entity consistent with all applicable HITECH requirements.

2.11 Comply with any other applicable PSR mandates as in effect or as amended subsequent to execution of this Addendum. For purposes of interpretation, all such mandates are incorporated herein by reference.

2.12 Comply with all state laws that are more restrictive than the PSRs including, without limitation, state laws that create special protections for PHI relating to behavioral health, communicable disease, or genetic testing, diagnosis and treatment.

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

Except as otherwise limited or restricted in the Principal Agreement or this Addendum, Business Associate may:

3.1 Use PHI for its proper management and administration or to carry out its legal responsibilities.

3.2 Disclose PHI for its proper management and administration, provided that such 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 the business Associate of any instances of which it is aware (as provided in the PSRs) in which the confidentiality of the information has been breached.

3.3 Use PHI to provide data aggregation services relating to Covered Entity's Health Care Operations, if and as requested by Covered Entity.

3.4 Use PHI to report violations of law to appropriate Federal and State authorities, consistent with the PSRs.

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

4.1 NPP Limitations. Covered Entity shall notify Business Associate of any limitations in Covered Entity's notice of privacy practices, to the extent such limitations may affect Business Associate's use or disclosure of PHI. Business Associate acknowledges that such notice may be in the form of an update to Covered Entity's website, online at <http://www.covenanthealthcare.com/documents/PrivacyPolicyNotice.pdf>.

4.2 Authorization Restrictions/Revocation. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an

Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

4.3 Confidential Communications or Restrictions. Covered Entity shall notify Business Associate of any agreement to engage in confidential communications or to restrict the use or disclosure of PHI as provided in the PSRs, to the extent such confidentiality or restriction agreements may affect Business Associate's use or disclosure of the affected Individuals' PHI.

4.4 Use or Disclosure in Violation of PSRs. Other than as provided in Section 3 above, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the PSRs if done by Covered Entity.

## **5. Miscellaneous Provisions**

5.1 Communications and Training. Without limitation on its other obligations described in Section 2 above, Business Associate represents and warrants that Business Associate's Related Parties who may provide services or perform functions or activities in connection with the Principal Agreement or this Addendum will be appropriately informed of the terms and conditions of this Addendum and trained as required by the PSRs to enable Business Associate and its Related Parties to assure compliance with the PSRs and this Addendum. At a minimum, such training shall occur upon hire or assignment to provide services or perform functions or activities under the Principal Agreement, and annually thereafter; shall be documented with such documentation maintained for a minimum of six (6) years after the training; and shall include documentation of the Related Parties' commitment to comply with the PSRs and Business Associate's privacy and security policies.

5.2 Breach. If Covered Entity or Business Associate becomes aware of an activity or practice by the other Party that constitutes a material breach or violation of that Party's obligations under this Addendum, the non-breaching Party shall seek the breaching Party's cooperation in promptly curing the breach or ending the violation. If such efforts are not completely successful, the non-breaching Party shall (i) terminate this Addendum (and the Principal Agreement if necessary to assure compliance with the PSRs); or (ii) if neither cure nor termination is feasible, notify the Secretary (or his or her designee) of the breach or violation.

5.3 Amendment. The Parties shall in good faith and without undue delay negotiate any amendments to this Addendum as may be required for either to comply with the PSRs, or to address changes in their relationship created by amendments to the PSRs but unanticipated at the time of execution of this Addendum.

5.4 Indemnification. Business Associate shall indemnify, defend, and hold harmless Covered Entity and its trustees, directors, officers, employees, agents, and members of its workforce (Covered Entity's "Related Parties") from and against any and all claims, demands, suits, actions, costs (including reasonable attorneys' fees), loss, liability, or expense incurred as a result of any breach of its obligations under this Addendum. For purposes of this Section 5.4, "breach" may occur, by way of illustration only, by negligence, intentional acts, errors or omissions by Business Associate or any of its Related Parties. Covered Entity shall promptly

notify Business Associate of its receipt of a written threat of or actual claim, demand, suit, or action; and shall tender its defense to Business Associate as a condition of the indemnification set forth herein.

5.5 No Third-Party Beneficiaries. This Addendum is entered into solely for the benefit of Covered Entity and Business Associate and does not and shall not be construed to confer any right, benefit, or remedy on any third party, including without limitation any Individual.

5.6 Term and Termination

(a) This Addendum shall remain in effect so long as the Principal Agreement remains in effect. Termination or expiration of the Principal Agreement shall automatically terminate this Addendum subject to the survival provisions specified in Paragraphs 5.6(b)-(c) below.

(b) Upon termination or expiration of the Principal Agreement under any circumstance, Business Associate shall, if feasible, return or destroy all PHI received from Covered Entity, or created or received by Business Associate (or Business Associate's Related Parties) on behalf of Covered Entity. Neither Business Associate nor its Related Parties will retain any copies of such PHI unless they determine and Covered Entity agrees that return or destruction is infeasible, in which case Business Associate (and its Related Parties, if and to the extent applicable), shall extend the protections of this Addendum to the information and limit further uses and disclosures to those purposes that make the return or destruction infeasible.

(c) Business Associate's obligations with respect to PHI retained following expiration or termination of the Principal Agreement or this Addendum shall survive such expiration or termination until all such PHI is returned to Covered Entity or destroyed in such a manner as to render such PHI "secured" pursuant to guidance issued from time to time by the Secretary.

5.7 No Further Revisions. All Provisions of the Principal Agreement not addressed in this Addendum shall remain in full force and effect. To the extent of any inconsistency between the Principal Agreement and this Addendum, the terms and conditions of this Addendum shall control.

In witness whereof, the Parties have executed this Addendum through their respective authorized representatives.

**Covered Entity:**

By: \_\_\_\_\_

Signature: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**Business Associate:**

By: \_\_\_\_\_

Signature: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**Acknowledgement:**

The undersigned is **Business Associate's security official**, as referenced in 45 CFR § 164.308(a)(2); has reviewed this Addendum; and hereby certifies Business Associate's compliance with its terms and conditions relevant to health information security.

Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Title: \_\_\_\_\_