**HIPAA Business Associate Agreement Example**

**INTRODUCTION AND DEFINITIONS**

1. PREAMBLE

A-1 Pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as amended

, [CUSTOMER] (Covered Entity) and [OTHER ENTITY], or any of its corporate affiliates (Business Associate), a [STATE] corporation, enter into this Business Associate Agreement (Agreement) as of [DATE] of [YEAR] (Effective Date) that addresses the HIPAA requirements with respect to “business associates,” as defined under the privacy, security, breach notification, and enforcement rules at 45

C.F.R. Part 160 and Part 164 (HIPAA Rules). A reference in this AGREEMENT to a section in the HIPAA Rules mean the section as in effect or as amended on the date this agreement is signed.

A-2 This AGREEMENT is intended to ensure that Business Associate will establish and implement appropriate safeguards for the Protected Health Information (PHI) that Business Associate may receive, create, maintain, use, or disclose in connection with the functions, activities, and services that Business Associate performs for Covered Entity. The functions, activities, and services that Business Associate performs for Covered Entity are defined in [UNDERLYING

AGREEMENT] (Underlying Agreement).

A-3 Unless the context clearly indicates otherwise, the following terms in this Agreement shall have the same meaning as those terms in the HIPAA Rules:

* Covered Entity
* Business Associate
* Electronic Protected Health Information (ePHI)
* [KEYWORD]
* [KEYWORD]

A-4 The AGREEMENT will only be applicable to the extent that the Business Associate has access to PHI that is provided by Covered Entity in the course of performing the Services under the Agreement.

A-5 A reference in this AGREEMENT to the Privacy Rule means the Privacy Rule, in conformity with the regulations at 45 C.F.R. Parts 160-164 (Privacy Rule) as interpreted under applicable regulations and guidance of general application published by HHS, including all amendments thereto for which compliance is required, as amended by the HITECH Act, ARRA, and the HIPAA Rules.

1. OBLIGATIONS OF BUSINESS ASSOCIATE

B-1 Business Associate agrees not to use or disclose PHI, other than as permitted or required by this

AGREEMENT or as permitted or required by law. Covered Entity represents that Business Associate’s use of any PHI provided by Covered Entity to Business Associate under the Agreement may be used by Business Associate for purposes of performing its services under the Agreement.

B-2 Business Associate shall use appropriate safeguards and comply with the requirements of the Security Rule to prevent the use or disclosure of PHI other than as permitted by this Agreement. Business Associate shall document and keep current its policies to safeguard PHI, and will provide evidence of such policies to Covered Entity within [TIMEFRAME] of receipt of a request.

B-3 Business Associate agrees to make its internal practices, books, and records, including policies and procedures regarding PHI, relating to the use and disclosure of PHI and breach of any unsecured PHI received from Covered Entity, or created or received by the Business Associate on behalf of Covered

Entity, available to the Secretary for the purpose of Covered Entity or the Secretary determining compliance with the Privacy Rule. Business Associate agrees to make available to Covered Entity, on the provision of not less than [DAYS] written notice, all relevant information necessary to demonstrate compliance with this Agreement, or allow for and contribute to an audit, by Covered Entity, or an auditor mandated by the Covered Entity, in relation to the processing of the PHI in accordance with the Agreement. Any audit under this section will be subject to the following conditions [LIST OUT CONDITIONS]

B-4 Business Associate agrees to report to Covered Entity any Breach of Unsecured PHI of which it becomes aware as soon as reasonably practical, but no more than within [TIMELINE] after discovery, as defined by the HITECH Act (on the first day of discovery). Such notice shall include, to the extent such information is available to Business Associate, the identification of each individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed in connection with such breach. In addition, Business Associate shall provide any additional information reasonably requested by Covered Entity for purposes of investigating the Breach and any other available information that Covered Entity is required to include to the individual under 45 C.F.R. § 164.404(c) at the time of notification or promptly thereafter as information becomes available.

B-5 Business Associate agrees, if applicable, to require that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same or similar restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.

B-6 Business Associate agrees that when requesting PHI in accordance with 45 C.F.R. § 164.502(b)(1), such request shall be to the minimum extent necessary to accomplish the intended purpose.

B-7 Business Associate agrees to maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy Covered Entity’s obligations under

45 C.F.R. § 164.528.

B-8 Business Associate will notify Covered Entity if it becomes aware of an Individual’s request to amend, modify, or restrict access to PHI, and Covered Entity will be responsible for fulfilling the request.

If feasible, based on the nature of the services provided and Business Associate’s access to the PHI, upon request from Covered Entity, Business Associate agrees to assist Covered Entity in fulfilling its obligation to comply with such individual’s request.

B-9 Business Associate agrees to make any amendments to PHI as directed or agreed to by the

Covered Entity pursuant to 45 C.F.R. § 164.526, or allow Covered Entity to make changes, and will take other reasonable measures as necessary and appropriate to satisfy Covered Entity’s obligations under HIPAA.

1. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

C-1 Business Associate agrees to receive, create, use, or disclose PHI only in a manner that is consistent with this AGREEMENT, the Privacy Rule, or Security Rule and only in connection with providing services to Covered Entity; provided that the use or disclosure would not violate the Privacy Rule, including 45 C.F.R. § 164.504(e), if the use or disclosure would be done by Covered Entity.

C-2 Business Associate may use or disclose PHI as required by law and may de-identify or anonymize PHI and use such it to the extent permitted by law or the regulation.

C-3 Business Associate agrees to limit any requests for, or disclosure of, PHI to the minimum necessary for Business Associate to fulfil its obligations under the Agreement. This should not violate Subpart E of 45 C.F.R. Part 164 if done by the Covered Entity.

1. PROHIBITED USES AND DISCLOSURES.

D-1 Business Associate shall not transmit, to any Individual for whom Business Associate has PHI, any communication about a product or service that encourages the recipient of the communication to purchase or use that product or service except as expressly agreed by the parties in this Agreement or with the individual. Business Associate shall not sell PHI or receive any direct or indirect compensation in exchange for PHI, except as expressly agreed by the parties in this Agreement.

D-2 As applicable, upon request from Covered Entity, Business Associate shall abide by a request from an Individual pursuant to 45 C.F.R. § 164.522(a) to refrain from making certain uses or disclosures of the Individual’s PHI.

1. OBLIGATIONS OF COVERED ENTITY

E-1 Covered Entity shall provide Business Associate with the Notice of Privacy Practices that Covered

Entity establishes in accordance with the Privacy Rule, as well as any changes or limitations to such notice(s) under 45 C.F.R. § 164.520, to the extent that such changes or limitations may affect Business Associate’s use or disclosure of PHI.

E-2 Covered Entity shall notify Business Associate of any changes in or revocation of permission by an individual to use or disclose PHI, if such change or revocation may affect Business Associate’s permitted or required uses and disclosures of PHI under this AGREEMENT.

E-3 Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that

Covered Entity has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate’s use or disclosure of PHI under this Agreement.

E-4 Covered Entity is responsible for ensuring the security of any PHI as it is being disclosed to Business Associate, including the use of encryption in transit. Also, the Covered Entity agrees to mitigate, to the extent practical, any harmful effect that is known to Covered Entity as a result of a use or disclosure of PHI.

E-5 Covered Entity acknowledges that Business Associate has not requested, does not need, and shall not request access to PHI in performing its obligations under the Agreement, and Covered Entity agrees, in accordance with its requirements under HIPAA, to limit the disclosure of PHI hereunder, and only to disclose to Business Associate the Minimum Necessary in order for Business Associate to perform its Services under the Agreement. In the event that Business Associate is notified by Covered Entity that Covered Entity has inadvertently provided PHI to Business Associate, Business Associate shall, at Covered Entity’s written request, not use or disclose such PHI in any manner and shall promptly follow

Covered Entity’s reasonable instructions regarding such PHI.

E-6 Covered Entity represents that it has all necessary authorizations and rights to share and disclose any PHI to Business Associate and that Business Associate is permitted to use same for the purposes of the Agreement. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy and Security Rule if done by Covered Entity.

1. COMPLIANCE WITH SECURITY RULE

F-1 Business Associate shall comply with the HIPAA Security Rule, which shall mean the Standards for

Security of Electronic Protected Health Information at 45 C.F.R. Part 160 and Subparts A and C of Part

164, as amended by ARRA and the HITECH Act.

F-2 In accordance with the Security Rule, Business Associate agrees to:

(a) Implement the administrative, physical, and technical safeguards to reasonably and appropriately protect the confidentiality, integrity, security, and availability of the PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity as required by the Security Rule.

(b) Require that any agent, including a Subcontractor, to whom it provides such PHI agrees to implement reasonable and appropriate safeguards to protect the PHI.

(c) Report to the Covered Entity any Security Incident of which it becomes aware.

1. TERM AND TERMINATION OF AGREEMENT

G-1 This AGREEMENT shall be in effect as of [DATE], and shall terminate on the earlier of the date that:

(a) Either party terminates for cause as authorized under Section G-2.

(b) All of the PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity. The obligations of Business Associate under this Section G shall survive the termination of this AGREEMENT.

G-2 Upon either party’s knowledge of material breach by the other party, the non-breaching party shall provide an opportunity for the breaching party to cure the breach, end the violation, or terminate the AGREEMENT. If the breaching party does not cure the breach or end the violation within a reasonable timeframe not to exceed [NUMBER] days from the notification of the breach, or if a material term of the AGREEMENT has been breached and a cure is not possible, the non-breaching party may terminate this AGREEMENT and the [UNDERLYING AGREEMENT], upon notice to the other party.

G-3 Upon termination of this AGREEMENT for any reason, the parties agree that the Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

(a) Retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities.

(b) Return or destroy the remaining PHI that the Business Associate still maintains in any form.

(c) Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to PHI to prevent use or disclosure of the PHI for as long as Business Associate retains the PHI.

(d) Destroy the PHI 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.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date written.

[COVERED ENTITY]

Name: [CE REPRESENTATIVE]

Title:

Date:

[BUSINESS ASSOCIATE]

Name: [BA REPRESENTATIVE]

Title:

Date: