

## BUSINESS ASSOCIATE ADDENDUM

THIS BUSINESS ASSOCIATE ADDENDUM (this “Addendum”), effective as of \_\_\_\_\_, 2011 (“Effective Date”), is entered into by and between the American Diabetes Association, Inc. (the “Business Associate”), and \_\_\_\_\_, (the “Covered Entity”) (each a “Party” and collectively the “Parties”).

WHEREAS, the Parties have entered into an agreement dated \_\_\_\_\_, 2011, for the use of Business Associate’s Chronicle Diabetes Software for the documentation of Covered Entity’s diabetes patient education record and Business Associate’s Program Management System for submission of Covered Entity’s required reports and applications for achieving and maintaining Recognized program status (the “Agreement”), under which the Covered Entity discloses Protected Health Information (individually identifiable health information of patients, as defined in 45 C.F.R. § 160.103) to the Business Associate for the purposes and obligations described below;

WHEREAS, the Business Associate creates, receives, uses or discloses Protected Health Information in its performance of the obligations described below;

WHEREAS, both Parties desire to meet their obligations under: (i) the Standards for Privacy of Individually Identifiable Information (“Privacy Regulation”) and the Security Standards (“Security Regulation”) published by the U.S. Department of Health & Human Services (“DHHS”) at 45 CFR parts 160 through 164 under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”); and (ii) the additional Privacy and Security Regulation requirements pursuant to Subtitle D of the Health Information Technology for Economic and Clinical Health Act (“HITECH”), including 45 CFR Sections 164.308, 164.310, 164.312, and 164.136, as amended from time to time (the “HITECH Standards”); and

WHEREAS, this Addendum sets forth the terms and conditions pursuant to which Protected Health Information that is received by, the Business Associate from or on behalf of the Covered Entity, will be handled between the Business Associate and the Covered Entity and with third parties during the term of their Agreement and after its termination.

NOW, THEREFORE, in consideration of the foregoing and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledges, the Parties hereby agree as follows:

### **1. DEFINITIONS.**

1.1 Citation to CFR. Regulatory citations in this Addendum are to the United States Code of Federal Regulations (“CFR”), as promulgated, interpreted, and amended from time to time by DHHS, for so long as such regulations are in effect.

1.2 Definitions under Privacy or Security Regulation. Unless otherwise specified in this Addendum, all terms not otherwise defined will have the meaning established for purposes of parts 160 through 164 of Title 45 of the CFR, as amended from time to time.

## **2. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION**

2.1 Services. Pursuant to the Agreement, the Business Associate provides services or goods for the Covered Entity that involves the use and disclosure of Protected Health Information. Except as otherwise specified herein, the Business Associate may make any and all uses of Protected Health Information necessary to perform its obligations under the Agreement, provided that such use or disclosure of protected health information would not violate the Privacy Regulation if done by the Covered Entity or the minimum necessary policies and procedures of the Covered Entity. All other uses not authorized by this Addendum or required by law are prohibited. Moreover, Business Associate may disclose Protected Health Information for the purposes authorized by this Addendum only, (i) to its employees, subcontractors and agents, in accordance with Section 3.1(f), (ii) as directed by the Covered Entity, or (iii) as otherwise permitted by the terms of this Addendum including, but not limited to, Section 2.2(b) below.

2.2 Business Activities of the Business Associate. Unless otherwise limited herein, the Business Associate may:

- a. Use the Protected Health Information in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of the Business Associate provided that such uses are permitted under state and federal confidentiality laws.
- b. Disclose the Protected Health Information in its possession to third parties for the purpose of its proper management and administration or to fulfill any present or future legal responsibilities of the Business Associate, if (i) the disclosures are required by law; (ii) the disclosures do not require an authorization or an “opportunity to agree”; or (iii) the Business Associate has received from the third party written reasonable assurances regarding its confidential handling of such Protected Health Information as required under 45 C.F.R. §§ 164.308(b)(1) and 164.504(e)(4).

2.3 Additional Activities of Business Associate. The Business Associate may also:

- a. At the request of the Covered Entity, aggregate the Protected Health Information in its possession with the Protected Health Information of other covered entities that the Business Associate has in its possession through its capacity as a business associate to said other covered entities provided that the purpose of such aggregation is to provide the Covered Entity with data analyses relating to the Health Care Operations of the Covered Entity. Under no circumstances may the Business Associate disclose Protected Health Information of one Covered Entity to another Covered Entity absent the explicit authorization of the Covered Entity.
- b. At the request of the Covered Entity, de-identify any and all Protected Health Information provided that the de-identification conforms to the requirements of 45 C.F.R. § 164.514(b), and further provided that the Covered Entity maintains any documentation required by 45 C.F.R. § 164.514(b) which may be in the form of a

written assurance from the Business Associate. Pursuant to 45 C.F.R. § 164.502(d)(2), de-identified information does not constitute Protected Health Information and is not subject to the terms of this Addendum.

### **3. RESPONSIBILITIES WITH RESPECT TO PROTECTED HEALTH INFORMATION**

3.1 Privacy Responsibilities of the Business Associate. With regard to its use or disclosure of Protected Health Information, the Business Associate will:

- a. Request from the Covered Entity, access, and disclose to its subcontractors, agents or other third parties, only the minimum amount of Protected Health Information necessary to perform or fulfill a specific function required or permitted under this Addendum or the Agreement.
- b. Use or disclose the Protected Health Information only as permitted or required by this Addendum or as otherwise required by law.
- c. Report to the designated Privacy Officer of the Covered Entity, in writing, any use or disclosure of the Protected Health Information that is not permitted or required by this Addendum of which Business Associate becomes aware within 5 business days of the Business Associate's discovery of such unauthorized use or disclosure.
- d. Establish procedures for mitigating, to the greatest extent possible, any deleterious effects from any improper use or disclosure of Protected Health Information that the Business Associate reports to the Covered Entity.
- e. Implement appropriate administrative, technical and physical safeguards to maintain the security of the Protected Health Information and to prevent its unauthorized use or disclosure.
- f. Require all its subcontractors and agents that receive or use, or have access to Protected Health Information under this Addendum to agree to the same restrictions and conditions on the use or disclosure of Protected Health Information that apply to the Business Associate pursuant to this Addendum.
- g. Make available all records, books, agreements, policies and procedures relating to the use or disclosure of Protected Health Information to the Covered Entity, or at the Covered Entity's request, to the Secretary of DHHS, in a time and manner designated by the Secretary, for purposes of determining the Covered Entity's compliance with the Privacy Regulation, subject to attorney-client and other applicable legal privileges.
- h. Upon prior written request, make available during normal business hours at Business Associate's offices all records, books, agreements, policies and procedures relating to the use or disclosure of Protected Health Information to the

Covered Entity within 15 days for purposes of enabling the Covered Entity to determine the Business Associate's compliance with the terms of this Addendum.

- i. Within 30 days of receiving a written request from the Covered Entity, provide to the Covered Entity such information as is requested by the Covered Entity to permit the Covered Entity to respond to a request by an individual for an accounting of the disclosures of the individual's Protected Health Information in accordance with 45 C.F.R. § 164.528.
- j. Document such 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 C.F.R. § 164.528.

3.2 HITECH Act and Security Responsibilities of the Business Associate. Notwithstanding any other provision in the Agreement or this Addendum, no later than February 17, 2010, unless a separate effective date is specified by law or the Agreement or this Addendum for a particular requirement (in which case the separate effective date will be the effective date for that particular requirement), the Business Associate will comply with the HITECH Standards. The Parties recognize that additional regulations and guidance documents may be issued implementing and interpreting HITECH during the term of the Agreement. The Business Associate will use reasonable efforts to comply with all applicable requirements of such additional regulations and guidance as they become effective, and agrees that to the extent such regulations or guidance require the Covered Entity to impose such requirements on the Business Associate, they are deemed imposed as and when they become effective. The Business Associate will further:

- a. Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Electronic Protected Health Information (as defined in 45 C.F.R. § 160.103) that it creates, receives, maintains or transmits on behalf of Covered Entity, and more specifically to secure all Electronic Protected Health Information with technologies and methodologies, including encryption, that render such information "secured" as defined in the guidance issued in 74 Fed. Reg. 19006 (April 27, 2009), pursuant to HITECH. Any Protected Health Information used, disclosed or maintained by the Business Associate that is not encrypted or destroyed will be deemed "Unsecured Protected Health Information."
- b. Require that any agent, including a subcontractor, to whom it provides Protected Health Information implement reasonable and appropriate safeguards to protect it, including but not limited to encryption that renders such information as "secured" as defined above.
- c. Notify the Covered Entity as soon as possible, but no later than the 5<sup>th</sup> day on which a security breach is known by Business Associate or an employee, officer or agent of Business Associate other than the person committing the breach, or as soon as possible following the first business day on which Business Associate or an employee, officer or agent of the Business Associate other than the person

committing the breach should have known by exercising reasonable diligence of such breach. “Security Breach” as used herein is defined as an acquisition, access, use, or disclosure of unsecured Electronic Protected Health Information in a manner not permitted under the HIPAA Privacy Rule. Notification will be made to Covered Entity via written notice as per section 7.4 of this Addendum.

- d. Report promptly to the Covered Entity any Security Incident, as defined in Section 164.304 of the Security Regulation, of which it becomes aware. However, the Business Associate will not be obliged to report an immaterial incident consisting solely of an unsuccessful attempt to improperly access information stored in systems under the Business Associate’s control.
- e. Establish procedures for mitigating, to the greatest extent possible, any deleterious effects from any improper breach to the security, confidentiality, integrity or availability of unsecured Electronic Protected Health Information that Business Associate knows of and reports to the Covered Entity as described above.

3.3 Responsibilities of the Covered Entity. With regard to the use or disclosure of Protected Health Information by the Business Associate, the Covered Entity will:

- a. Obtain any consent or authorization that may be required by 45 CFR §§ 164.506 and 164.508, or applicable state law, prior to furnishing the Business Associate the Protected Health Information pertaining to such individual.
- b. Notify the Business Associate of any limitation in the Covered Entity’s notice of privacy practices to the extent that such limitation may affect the Business Associate’s use or disclosure of Protected Health Information.
- c. Not furnish Protected Health Information to the Business Associate that is subject to any arrangements permitted or required of the Covered Entity under the Privacy Regulation, Security Regulation, or HITECH Standards that may impact in any manner the use or disclosure of Protected Health Information by the Business Associate under this Addendum and the Agreement, including but not limited to restrictions on use or disclosure of Protected Health Information as provided for in 45 CFR § 164.522 and agreed to by the Covered Entity.

3.4 Responsibilities of the Parties with Respect to Breach Notification. As of the effective compliance date for the HITECH Standards as they apply to Security Breaches (as contemplated by Section 3.2(c) herein), the Parties with comply with the HITECH Standard related to the notification of affected individuals in the event of a Security Breach of Protected Health Information (the “Breach Notification Rule”).

- a. Except as provided by 45 CFR § 164.412, the Business Associate will give the Covered Entity notice of any breach of Unsecured Protected Health Information as required by Sections 3.2(c) and 7.4 of this Addendum.
- b. Such notice will be written in plain language and will include, to the extent possible or available, the following: (i) the identification of all individuals whose

Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during the breach; (ii) a brief description of what happened, including the date of the breach and the date of the discovery of the breach; (iii) a description of the types of Unsecured Protected Health Information that were involved in the breach; (iv) any steps that individuals who were subjects of the breach should take to protect themselves from potential harm that may result from the breach; (v) a brief description of what Business Associate is doing to investigate the breach, to mitigate the harm to affected individuals, and to protect against further Breaches; and (vi) contact procedures for affected individuals to ask questions or learn additional information, including a toll-free telephone number, an email address, a website, or postal address.

- c. Notwithstanding the provisions of this Section 3.4 and if a law enforcement official states to the Business Associate that notification of a breach would impede a criminal investigation or cause damage to national security, then: (i) the notification will be delayed for the time period specified by the official if the official's statement is in writing and specifies the time for which a delay is required; or (ii) if the official's statement is made orally, the Business Associate will document the oral statement, including the identity of the official making the statement, and delay the breach notification for no longer than 30 days from the date of the oral statement, unless the official submits a written statement during that time period
- d. Cooperate with the Covered Entity as needed to further investigate and evaluate any Security Breach involving the Business Associate or of which the Business Associate has become aware.
- e. In the event of impermissible use or disclosure is made by the Business Associate or any subcontractor or agent of Unsecured Protected Health Information that, in the reasonable judgment of the Covered Entity, requires a Breach Notification, the Business Associate (or subcontractor or agent) will, at the Covered Entity's direction, provide such Breach Notification in accordance with this Section 3.4 and the HITECH Standards.
- f. The Party responsible for the breach of Unsecured Protected Health Information will be responsible for payment of all actual costs associated with the breach, including, but not limited to, costs of notifying affected individuals, credit monitoring (where applicable), and other efforts to mitigate the harm to affected individuals.

#### **4. ADDITIONAL RESPONSIBILITIES OF THE PARTIES WITH RESPECT TO PROTECTED HEALTH INFORMATION**

4.1 Responsibilities of the Business Associate with Respect to Handling of Designated Record Set. In the event that the Parties mutually agree in writing that the Business Associate

will maintain Protected Health Information in Designated Record Sets, the Business Associate will:

- a. At the request of, and in the time and manner designated by the Covered Entity, provide access to the Protected Health Information to the Covered Entity or the individual to whom such Protected Health Information relates, or his or her authorized representative, in order to meet a request by such individual under 45 C.F.R. § 164.524.
- b. At the request of, and in the time and manner designated by the Covered Entity, make any amendment(s) to the Protected Health Information that the Covered Entity directs pursuant to 45 C.F.R. § 164.526; provided, however, that the Covered Entity makes the determination that the amendment(s) are necessary because the Protected Health Information that is the subject of the amendment(s) has been, or could foreseeably be, relied upon by the Business Associate or others to the detriment of the individual who is the subject of the Protected Health Information to be amended.

4.2 Responsibilities of the Covered Entity with Respect to the Handling of the Designated Record Set. In the event that the Parties mutually agree in writing that the Business Associate will maintain Protected Health Information in Designated Record Sets, the Covered Entity will:

- a. Notify the Business Associate, in writing, of any Protected Health Information that Covered Entity seeks to make available to an individual pursuant to 45 CFR § 164.524 and the time, manner and form in which the Business Associate will provide such access.
- b. Notify the Business Associate, in writing, of any amendment(s) to the Protected Health Information in the possession of the Business Associate that the Business Associate will make and inform the Business Associate of the time, form and manner in which such amendment(s) will be made.

## **5. REPRESENTATIONS AND WARRANTIES OF THE PARTIES**

5.1 Workforce Informed of Addendum Terms. All of each Party's employees, agents, representatives and members of its respective workforce whose services may be used to fulfill obligations under this Addendum are or will be appropriately informed of the applicable terms and conditions of this Addendum and are under legal obligation to each Party, respectively, by contract or otherwise, sufficient to enable each Party to comply fully with all applicable provisions of this Addendum.

5.2 Reasonable Cooperation among the Parties. Each Party will reasonably cooperate with the other Party in the performance of the mutual obligations under this Addendum.

5.3 Prepared to Comply with HIPAA/HITECH Requirements. Each Party represents and warrants that it has or is prepared to comply with the applicable provisions of this Addendum on or before: (i) April 14, 2003 (Privacy Regulation), April 20, 2005 (Security Regulation), and

February 17, 2010 (HITECH Standards), if the Agreement was in effect on such dates; or (ii) the Effective Date, if no Agreement was in effect prior to the Effective Date.

## **6. TERMS AND TERMINATION**

6.1 Term. This Addendum will become effective on the Effective Date and will continue in effect until all obligations of the Parties have been met, unless terminated as provided in this Section 6. In addition, certain provisions and requirements of this Addendum will survive its expiration or other termination in accordance with Section 7.1 herein.

6.2 Termination by the Parties. As provided for under 45 CFR § 164.504(e)(2)(iii), the Covered Entity or Business Associate may immediately terminate the Agreement and this Addendum if the non-breaching Party makes the determination that the other Party has breached a material term of this Addendum. Alternatively, the non-breaching party may choose to: (i) provide the breaching Party with 10 days written notice of the existence of an alleged material breach; and (ii) afford the breaching Party an opportunity to cure said alleged material breach upon mutually agreeable terms. Nonetheless, in the event that mutually agreeable terms cannot be achieved within 10 days, the breaching Party must cure said breach to the satisfaction of the non-breaching Party within a reasonable and mutually agreed upon time period. Failure to cure in the manner set forth in this Section 6.2 is grounds for the immediate termination of the Agreement and this Addendum. If neither termination nor cure is feasible, the non-breaching Party will report the violation to the Secretary of DHHS.

6.3 Automatic Termination. This Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Agreement.

6.4 Effect of Termination. Upon the event of termination pursuant to this Section 6, the Business Associate will return or destroy all Protected Health Information, including Electronic Protected Health Information, pursuant to 45 CFR § 164.504(e)(2)(I), if it is feasible to do so. Prior to doing so, the Business Associate further will recover any Protected Health Information in the possession of its subcontractors or agents. If it is not feasible for the Business Associate to return or destroy said Protected Health Information, the Business Associate will notify the Covered Entity in writing. Said notification will include: (i) a statement that the Business Associate has determined that it is infeasible to return or destroy the Protected Health Information in its possession, and (ii) the specific reasons for such determination. In such event, the Business Associate will extend any and all protections, limitations and restrictions contained in this Addendum to the Business Associate's use or disclosure of any Protected Health Information retained after the termination of this Addendum or the Agreement, and to limit any further uses or disclosures to the purposes that make the return or destruction of the Protected Health Information infeasible. If it is infeasible for the Business Associate to obtain, from a subcontractor or agent any Protected Health Information in the possession of the subcontractor or agent, the Business Associate must provide a written explanation to the Covered Entity and require the subcontractors and agents to agree to extend any and all protections, limitations and restrictions contained in this Addendum to the subcontractors' or agents' use or disclosure of any Protected Health Information retained after the termination of this Addendum, and to limit any further uses or disclosures to the purposes that make the return or destruction of the Protected Health Information infeasible.

## 7. MISCELLANEOUS

7.1 Survival. The respective rights and obligations of the Business Associate and Covered Entity under the provisions of Sections 3.1, 3.2, 3.4 and 6.4, solely with respect to Protected Health Information that the Business Associate retains in accordance with Section 6.4 because it is not feasible to return or destroy such Protected Health Information, will survive termination of this Addendum indefinitely. In addition, Section 4 will survive termination of this Addendum, provided that the Covered Entity determines that the Protected Health Information being retained pursuant to Section 6.4 constitutes a Designated Record Set.

7.2 Change of Law. Each Party will notify the other within 90 days of any amendment to any provision of HIPAA or HITECH, or their implementing regulations, which such Party reasonably believes will materially alter either Party's or both Parties' obligations under this Addendum. Upon provision of such notice, the Parties will negotiate in good faith mutually acceptable and appropriate amendment(s) to this Addendum to give effect to such revised obligations; provided, however, that if the Parties are unable to agree on such amendment(s) within 90 days of the relevant change of law, either Party may terminate this Addendum consistent with Sections 6.2 and 6.4 herein.

7.3 Amendments; Waiver. This Addendum may not be modified, nor will any provision be waived or amended, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event will not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

7.4 Assignment of Rights and Delegation of Duties. This Addendum is binding upon and inures to the benefit of the Parties and their respective successors and permitted assigns. However, neither Party may assign any of its rights or delegate any of its obligations under this Addendum without the prior written consent of the other Party, which consent will not be unreasonably withheld or delayed. Assignments made in violation of this Section 7.4 will be null and void.

7.5 No Third Party Beneficiaries. Nothing express or implied in this Addendum is intended to confer, nor will anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

7.6 Notices. Any notices to be given will be made via fax or express courier to the address given below, except that notice of a Security Breach will also be given as provided in section 3.2(c) of this Addendum.

7.7 Interpretation. Any ambiguity in this Addendum and the Agreement will be resolved to permit Covered Entity to comply with the Privacy and Security Rules and the HITECH Act and applicable regulations and guidance documents.

7.8 Counterparts; Facsimiles. This Addendum may be executed in any number of counterparts, each of which will be deemed an original. Facsimile copies hereof will be deemed to be originals.

IN WITNESS WHEREOF, each of the undersigned has caused this Addendum to be duly executed in its name and on its behalf effective as of the Effective Date stated above herein.

**COVERED ENTITY**

**BUSINESS ASSOCIATE**

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

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

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

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

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

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

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

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