AT&T HIPAA BUSINESS ASSOCIATE AGREEMENT FOR SERVICES PROVIDED WITHOUT A SIGNED WRITTEN AGREEMENT

1. APPLICATION

a. For purposes of this Agreement, "Services" shall mean those products and services provided by AT&T to Customer pursuant to the terms of a Service Agreement. Services include "Mobility Applications." Mobility Application shall mean an application provided to Customer by AT&T that is resold or licensed to Customer by AT&T or an affiliate, agent or subcontractor of AT&T and which is provisioned over, or utilizes, AT&T wireless service. Neither Services nor Mobility Application include applications or services provided by a third party, regardless of whether such application or service utilizes AT&T wireless service.

b. Subject to more specific terms described in an applicable Service Guide or Service Publication, the terms of this BAA shall apply only to those Services where AT&T acts in the capacity of a Business Associate in the course of providing the Services.

c. By using the Services to transmit, store, access, manage or maintain Protected Health Information (PHI), Covered Entity acknowledges it is bound by this BAA.

2. BUSINESS ASSOCIATE OBLIGATIONS

a. Business Associate agrees to:

i. not Use or Disclose PHI in violation of this BAA, the Agreement or applicable law;

ii. use appropriate safeguards and security measures to prevent unauthorized Use or Disclosure of PHI;

iii. provide a written report to Covered Entity, within 5 days of verification, of any unauthorized Use or Disclosure of PHI. Business Associate's written report will, to the extent known, reflect:

a. the nature of the unauthorized Use or Disclosure;
b. the PHI used or disclosed; and
c. the corrective action Business Associate has or will take to prevent similar unauthorized Use or Disclosure in the future;

iv. report to Covered Entity, without undue delay, but in no event later than five (5) days of verification, any Breach of Unsecured PHI and cooperate with Covered Entity's investigation of the Breach and fulfilling Covered Entity's obligations under the HITECH Act and any other security breach notification laws. The Breach notification will, to the extent known, include the identity of each Individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such Breach;

v. report to Covered Entity, within 5 days of becoming aware, any successful Security Incident;

vi. report, upon Covered Entity's request, attempted but unsuccessful Security Incidents of which Business Associate becomes aware; provided that Covered Entity's request shall be made no more often than is reasonable based upon the relevant facts, circumstances and industry standards;

vii. require its agent(s) and subcontractor(s) who receive Covered Entity's PHI, whether it was received from, or created by Business Associate on behalf of Covered Entity, to agree in writing to substantially the same conditions and security measures agreed to by Business Associate under this BAA;

viii. make internal practices, books, and records, including policies and procedures, relating to the Use and Disclosure of PHI received from Covered Entity, or created by Business Associate on behalf of Covered Entity, available to the Secretary, in a time and manner as reasonably requested by or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule and the Security Rule;

ix. document Disclosures of PHI sufficiently to allow Covered Entity to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 C.F.R. § 164.528. Business Associate will provide Covered Entity, in a mutually agreeable time and manner, documentation necessary for Covered Entity to respond to a request by an Individual for an accounting of Disclosures of PHI by Business Associate. Under no circumstances will Business Associate be required to accept or respond to accounting requests made by Individuals; Covered Entity is responsible for responding to all such accounting requests;

x. provide Covered Entity access to PHI as required to meet the requirements under 45 C.F.R. § 164.524 and HITECH Act. Under no circumstances will Business Associate be required to accept or respond to requests for access to PHI made by Individuals; Covered Entity is responsible for receiving and processing all such requests from Individuals;

xi. make amendment(s) to PHI at the request, direction and agreement of Covered Entity (provided in accordance with 45 C.F.R. § 164.526), in the time and manner agreed to by the parties; and

xii. to the extent Business Associate specifically agrees in writing, carry out Covered Entity's obligations under Subpart E of 45 C.F.R. § 164, and comply with the requirements of Subpart E that would apply to Covered Entity in the performance of those obligations.

b. The parties acknowledge that:

i. Business Associate's ability to report on system activity including Security Incidents, is limited by, and to, the Services which Covered Entity has purchased;

.

ii. Business Associate has no obligation to report unsuccessful Security Incidents or to monitor Customer's Services other than as included with and permitted by those Services that the Customer purchases or those procedures separately agreed to in writing; and

iii. Business Associate has no obligation to report network security related incidents which occur on the AT&T managed network but do not directly involve Customer's PHI or BA - Related Services.

3. <u>PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE</u>

a. Business Associate may:

i. Use or Disclose PHI to perform functions and activities necessary to provide Services to the Covered Entity; provided that such Use or Disclosure does not violate the Privacy Rule, the Security Rule, HITECH, this BAA or the Agreement;

ii. Use or Disclose PHI to perform functions and activities necessary to provide Services to the Covered Entity;

iii. Disclose PHI for Business Associate's proper management, administration and legal responsibilities, if:

a. the Disclosures are required or permitted by law; or
b. reasonable assurances are obtained from the person to whom the information is disclosed that:

1. 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
2. it will notify the Business Associate of any breach of confidentiality with respect to the PHI of which it becomes aware.

iv. use PHI to provide data aggregation services to Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B), except as otherwise limited in this BAA.

4. OBLIGATIONS OF COVERED ENTITY

a. Covered Entity agrees to:

i. notify Business Associate of any limitation(s) in Covered Entity's Notice of Privacy Practices in accordance with 45 C.F.R. § 164.520, to the extent such limitation affect Business Associate's Use or Disclosure of PHI ("Changes to Privacy Practices").

ii. notify Business Associate of any changes in, or revocation of, permission by an Individual to Use or Disclose PHI, to the extent such changes affect Business Associate's Use or Disclosure of PHI.

iii. notify Business Associate of any restriction to the Use or Disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522 ("Use or Disclosure Restrictions"), to the extent such restrictions affect Business Associate's Use or Disclosure of PHI.

iv. not store, transmit or deliver to Business Associate any PHI in an unencrypted state without Business Associate's knowledge and express written consent. Covered Entity will encrypt PHI at rest in a manner consistent with guidelines established by the Secretary, except where the provision of the Services requires PHI to be unencrypted. If, however, Business Associate expressly undertakes the obligation to encrypt PHI on behalf of Covered Entity for any BA-Related Services, Business Associate's knowledge and consent under this provision will be presumed.

5. PERMISSIBLE REQUESTS BY COVERED ENTITY

Covered Entity will not ask Business Associate to Use or Disclose PHI in any manner that would not be permissible under the Privacy Rule or the Security Rule if done by Covered Entity.

6. TERM AND TERMINATION

a. **Term** This BAA will be effective when executed by both parties, and will terminate when:

i. Business Associate no longer provides BA-Related Services to Covered Entity; and

ii. All of the PHI 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, as provided in (d) below.

b. **Termination for Cause** When Covered Entity becomes aware of a material breach of this BAA by Business Associate, Covered Entity will either:

i. provide Business Associate an opportunity of at least 30 days to cure the breach or end the violation and if Business Associate does not cure the breach or end the violation within the cure period, terminate the Agreement for the affected BA-Related Services; or

ii. if cure is not possible, immediately terminate the Service Agreement(s) for the affected BA-Related Services.

c. **Cure of Non-material Breach** Covered Entity shall provide an opportunity for Business Associate to cure a non-material breach within a time mutually agreeable to the parties.

d. **Effect of Termination**

Upon termination of the affected Agreement for BA-Related Services for any reason, Business Associate will return or destroy all PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity, unless Business Associate determines that returning or destroying the PHI is infeasible, in which case, Business Associate will provide Covered Entity with written notice of the conditions that make return or destruction infeasible. In such case, the terms of this BAA will continue to protect the PHI and Business Associate will, for as long as it maintains such PHI, limit further Use and Disclosure to those purposes that make the return or destruction infeasible. This provision shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate.

7. GENERAL PROVISIONS

Amendment To the extent necessary to maintain compliance with the requirements of Use or Disclosure Restrictions, Changes to Privacy Practices, HIPAA, HITECH, the Privacy Rule, the Security Rule, the Electronic Transaction Standards and related regulations and technical pronouncements, the Parties agree to meet and negotiate appropriate amendments in good faith. This Addendum may not be amended unless in writing signed by the duly authorized representatives of the respective parties.

8. DEFINITIONS

The following definitions apply only to this BAA. In the event a term appears which is not defined here, it will have the meaning reflected in HIPAA, ARRA, HITECH, the Security Rule, the Privacy Rule or the Agreement.

a. **ARRA** means the American Recovery and Reinvestment Act of 2009.

b. **BA-Related Services** means Services where, in the course of providing the Services under the Agreement(s), AT&T acts as Business Associate.

c. **Breach** has the meaning stated in 45 C.F.R. § 164.402.

d. **Business Associate** means AT&T when it acts in the capacity of a "business associate" as defined in 45 C.F.R. § 160.103.

e. **C.F.R.** means the Code of Federal Regulations as amended and in effect at the relevant time.

f. **Covered Entity** means Customer when it is acting as a "covered entity" as defined in 45 C.F.R. § 160.103 and also when it is acting as business associate to a third party and AT&T is acting as the Business Associate.

g. **Disclose** or **Disclosure** has the meaning stated in 45 C.F.R. §160.103.

h. **Electronic Transaction Standards** means the standards defined by 45 C.F.R. Parts 160 and 162.

i. **HIPAA** means the Health Information Portability and Accountability Act of 1996, as amended from time to time and as codified at various places throughout the United States Code.

j. **HITECH Act** means the Health Information Technology for Economic and Clinical Health Act, as incorporated in the ARRA.

k. **Individual** has the meaning stated under the Privacy Rule, including, but not limited to, 45 C.F.R. §160.103, and includes a person who qualifies as a personal representative under 45 C.F.R. §164.502(g).

l. **Notice of Privacy Practices** means the Covered Entity's legally required notice of privacy practices for Protected Health Information required by 45 C.F.R. §164.520.

m. **Privacy Rule** means the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164 (Subparts A and E).

n. **Protected Health Information (PHI)** has the meaning stated in 45 C.F.R. § 160.103.

o. **Secretary** means the Secretary of the United States Department of Health and Human Services.

p. **Security Incident** has the meaning stated in 45 C.F.R. §164.304.

q. **Security Rule** means the Security Standards at 45 C.F.R. Part 160, Part 162 and Part 164.

r. **Services** means the products and services provided by AT&T to Customer under the terms of the Agreement

s. **Unsecured PHI** means Unsecured Protected Health Information as defined in §13402(h) of the ARRA.

t. **Use** has the meaning stated in 45 C.F.R. §160.103.