HIPAA BUSINESS ASSOCIATE AGREEMENT ("BAA") COVERING SERVICES PROVIDED TO CUSTOMERS WITHOUT A SIGNED BAA

WHEREAS, Cotiviti is in the business of providing software and licenses for the use of software to Customers under Underlying Agreement(s);

WHEREAS, Customers who make available, transfer and/or disclose confidential, individually identifiable health information ("PHI") to Cotiviti for the purpose of providing such software Services are deemed "Covered Entities" under HIPAA and Cotiviti is deemed a "Business Associate" under HIPAA;

WHEREAS, HIPAA requires that a Covered Entity and a Business Associate enter into a written agreement for the protection of PHI known as a "Business Associate Agreement" or "BAA";

WHEREAS, the parties desire to implement a BAA on the terms set forth herein when (a) Customer is acting as a Covered Entity and Cotiviti is acting as a Business Associate, and (b) the parties' Underlying Agreement(s) do not contain a written, signed BAA; and

WHEREAS, the parties agree to comply with applicable regulations governing the use and disclosure of PHI and Unsecured PHI, including the privacy regulations, 45 CFR Part 160 and 45 CFR Part 164, Subparts A and E ("Privacy Rule"), and the security regulations, 45 CFR Part 164, Subparts A and C ("Security Rule") issued pursuant to the Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by any other statute, rule and/or regulation, including Division A, Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub. L. No., 111-5) ("HITECH");

NOW THEREFORE, the parties agree as follows:

1. Application

Subject to more specific terms described in the Underlying Agreement(s), the terms of this BAA shall apply only to those Services where Cotiviti acts in the capacity of a Business Associate. In providing certain Services (such as deployment of software in an environment wholly controlled by Covered Entity), Cotiviti does not act in the capacity of a Business Associate. In the event that Customer purchases more than one Service from Cotiviti, Cotiviti may act in the capacity of a Business Associate for some Services, but not others. By using such Services and/or providing access to PHI to Cotiviti, Customer agrees to be bound by the terms of this BAA.

2. Business Associate Obligations.

2.1. Business Associate agrees to:

2.1.1 not Use or Disclose PHI in violation of this BAA, the Underlying Agreement(s) or applicable law;

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

2.1.3 provide a written report to Covered Entity, within five (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;

2.1.4 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;

2.1.5 report to Covered Entity any successful Security Incident within five (5) days of learning of such successful Security Incident, if the notice period falls on a weekend or public holiday, then the notice is due on the following next business day;

2.1.6 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; this section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice is required. "Unsuccessful Security Incidents" include, but are not limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, and denial of service attacks, so long as there is no unauthorized access, use or disclosure of electronic PHI. All reports of Breaches shall be made in compliance with 45 CFR §164.410.

2.1.7 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;

2.1.8 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;

2.1.9 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;

2.1.10 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;

2.1.11 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;

2.1.12 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; and

2.1.13 promptly forward any requests Business Associate receives from Individuals to Covered Entity for appropriate response.

2.2. The parties acknowledge that:

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

2.2.2 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

2.2.3. Business Associate has no obligation to report network security related incidents that do not directly involve Customer's PHI or Services.

3. <u>Permitted Uses and Disclosures by Business Associate</u>

3.1 Business Associate may:

3.1.1 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 Underlying Agreement(s);

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

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

3.1.3.1 the Disclosures are required or permitted by law; or

3.1.3.2 reasonable assurances are obtained from the person to whom the information is disclosed that:

(i) 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

(ii) it will notify the Business Associate of any breach of confidentiality with respect to the PHI of which it becomes aware; and

3.1.4 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

4.1. Covered Entity agrees to:

4.1.1. 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(s) affect(s) Business Associate's Use or Disclosure of PHI ("Changes to Privacy Practices");

4.1.2 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;

4.1.3. 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; and

4.1.4. 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.

4.1.5. ensure that no malicious software, virus, code or similar items are introduced into Business Associate's infrastructure, hardware, software, systems and networks (collectively, the "Business Associate Environment") by Customer, Customer Personnel or any other Customer entity, affiliate or subcontractor.

4.1.6 Acceptable Use. Covered Entity acknowledges and agrees that Business Associate does not monitor or police the content of communications or data of Covered Entity and/or its authorized end user transmitted through the Software (as define din the Master Service and License Agreement), and that Business Associate shall not be responsible for the content of any such communications or transmissions. Covered Entity shall use the software exclusively for authorized and legal purposes, consistent with all applicable laws and regulations, and as defined in the Documentation or Order Form. Covered Entity is solely responsible for making sure it has obtained permissions or authorizations to permit Business Associate to perform its obligations hereunder (for example, obtained third-party consent or authorization for the transmittal of any PHI that may be embedded in the data, content, and information processed through the Software). Covered Entity shall not: (i) reverse engineer, decompile, probe, scan, or attempt to discover any source code or underlying ideas or algorithms utilized in the Software; (ii) send or store infringing, unlawful, defamatory or libelous material; (iii) remove the copyright, trademark, or any other proprietary rights or notices included within the Software, or on and in the Documentation; (iv) copy, download, scrape, store, publish, transmit, transfer, distribute, broadcast, circulate, sub-license, bundle with other products, sell or otherwise use any portion of the Software, in any form or by any

means, except as expressly permitted by an applicable Order Form; or (v) engage in any activity that could reasonably be expected to interfere with or disrupt the Software (e.g., an activity that causes Cotiviti to be blacklisted by any internet service provider). Business Associate may remove any violating content posted or transmitted through the Software, without notice to Covered Entity. Business Associate may suspend or terminate any end user's access to the Software upon notice in the event that Business Associate reasonably determines that such user has violated the terms and conditions of this Agreement.

4.1.7 Security. In addition to any mutual obligations list in the underling Agreements, Covered Entity will not: (a) breach or attempt to breach the security of the Software or any network, servers, data, computers or other hardware relating to or used in connection with the Software, or any third-party that is hosting or interfacing with Business Associate; or (b) use or distribute through the Software any software, files or other tools or devices designed to interfere with or compromise the privacy, security, or use of the Software or the operations or assets of any other customer of Business Associate or any third party. Covered Entity will comply with the user authentication requirements for use of the Software. Covered Entity is solely responsible for monitoring its end user access to and use of the Software. Business Associate has no obligation to verify the identity of any person who gains access to the Software by means of an access ID. Any failure by any end user to comply with this agreement shall be deemed to be a material breach by Covered Entity, and Business Associate shall not be liable for any damages incurred by Covered Entity or any third-party resulting from such breach. Covered Entity must immediately take all necessary steps, including providing notice to Business Associate, to effect the termination of an access ID for any end user if there is any compromise in the security of that access ID or if unauthorized use is suspected or has occurred.

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.

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

6.1.1 Business Associate no longer provides Services to Covered Entity; and

6.1.2. 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 Section 6.5, below.

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

6.2.1 provide Business Associate an opportunity of at least thirty (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 Service Agreement(s) for the affected Services; or

6.2.2 if cure is not possible, immediately terminate the Underlying Agreement(s) for the affected Services.

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

6.4 Effect of Termination. Upon termination of the affected Underlying Agreement for any individual Service for any reason, Business Associate will return or destroy all PHI (or, in the case of a single Service, all PHI related to that Service) 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.

7.1 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, Business Associate will modify this BAA to comply with such changes. Such changes will become effective immediately upon posting of a revised version of this BAA by Business Associate. In the event Covered Entity does not agree to the provisions of the revised BAA posted by Business Associate, Customer shall promptly request Business Associate to begin negotiations for a written, signed BAA. The terms of the then-current posted version of this BAA shall continue to apply until such time as any negotiations for a written, signed BAA are concluded and a new BAA is executed by the parties.

7.2 Limitations of Liability and Damages

7.2.1 Limitation of Liability. IN NO EVENT WILL BUSINESS ASSOCIATE BE LIABLE TO COVERED ENTITY OR TO ANY THIRD PARTY FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR EXEMPLARY DAMAGES (WHETHER FORESEEABLE OR NOT, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOSS OF DATA, GOODWILL, PROFITS, INVESTMENTS, REPUTATION, USE OF MONEY OR USE OF FACILITIES; INTERRUPTION IN USE OR AVAILABILITY OF DATA; STOPPAGE OF OTHER WORK OR IMPAIRMENT OF OTHER ASSETS). THIS EXCLUSION OF DAMAGES APPLIES EVEN IF COVERED ENTITY HAS BEEN ADVISED OR IS OTHERWISE AWARE OF THE POSSIBILITY OF SUCH DAMAGES, AND HOWEVER THE DAMAGES HAVE ARISEN (WHETHER OUT OF THE PERFORMANCE OR NON-PERFORMANCE OF THIS BAA, THE SOFTWARE OR SERVICES; OR ANY CLAIM, CAUSE OF ACTION, BREACH OF CONTRACT OR EXPRESS OR IMPLIED WARRANTY UNDER THIS BAA OR ANY THEORY OF LAW SUCH AS MISREPRESENTATION, NEGLIGENCE, STRICT LIABILITY, OR OTHER TORT).

7.2.2 Limitation of Damages. TO THE FULLEST EXTENT PERMISSIBLE UNDER APPLICABLE LAW, BUSINESS ASSOCIATE'S ENTIRE LIABILITY ARISING OUT OF THIS BAA WILL IN NO EVENT EXCEED THE FEES PAID BY COVERED ENTITY TO BUSINESS ASSOCIATE UNDER THE UNDERLYING AGREEMENT(S) DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING COVERED ENTITY'S FIRST ASSERTION OF ANY CLAIM AGAINST BUSINESS ASSOCIATE, AND IN ANY EVENT WILL NOT EXCEED US$1,000,000, WHETHER OR NOT THE ACTION OR CLAIM IS BASED IN CONTRACT, MISREPRESENTATION, WARRANTY, INDEMNITY, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL THEORY. SUBJECT TO THE LIMITATIONS IN THIS SECTION 7, BUSINESS ASSOCIATE'S LIABILITY FOR COVERED ENTITY'S ASSOCIATE'S DIRECT DAMAGES ARISING

FROM BUSINESS ASSOCIATE'S BREACH OF THIS BAA AND/OR A SECURITY INCIDENT, WHERE THE ROOT CAUSE OF THE SECURITY INCIDENT AROSE FROM AN ACT OR OMISSION OF BUSINESS ASSOCIATE'S CONTRACTUAL OBLIGATIONS (AS DETERMINED BY AN INDEPENDENT INVESTIGATOR) WILL BE LIMITED TO (I) REASONABLE FEES AND EXPENSES COVERED ENTITY INCURS IN INVESTIGATING, RESPONDING TO, AND/OR MITIGATING THE SECURITY INCIDENT; AND/OR (II) FOR FINES, ASSESSMENTS, SANCTIONS, AND/OR CIVIL PENALTIES ASSESSED OR IMPOSED AGAINST COVERED ENTITY BY ANY GOVERNMENT AGENCY/REGULATOR.

7.2.3 For purposes of clarification, any obligations of Cotiviti under this Business Associate Agreement to defend, indemnify and hold harmless Customer shall not apply to Cotiviti to the extent that: (i) the Incident or Breach (as defined under this BAA) was caused by Customer's failure to meet its obligations under the Business Associate Agreement, the Agreement, or under the provisions of HIPAA and HITECH; (ii) Customer's costs and expenses are unreasonable; or (iii) Cotiviti did not have, and was not required to have, possession, custody, or control of the PHI involved in the Security Incident or Breach or (iv) Covered Entity is identified as the root cause of the incident by which Covered Entity's damages arise.

8. <u>Definitions.</u>

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 Underlying Agreement.

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

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

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

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

8.5 "**Covered Entit**y" 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 Cotiviti is acting as the Business Associate.

8.6 **"Customer"** means an individual or entity purchasing Services from Cotiviti.

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

8.8 "**Cotiviti"** means Cotiviti, Inc. and its affiliates who provide Services to Customers. Throughout the majority of this document, Cotiviti is referred to as Business Associate.

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

8.10 **"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.

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

8.12 **"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).

8.13 **"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.

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

8.15 **"Protected Health Information (PHI)"** has the meaning stated in 45 C.F.R. § 160.103. For purposes of this BAA, PHI includes electronic PHI ("ePHI").

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

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

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

8.19 **"Services"** means the products and services provided by Cotiviti to Customer under the terms of the Underlying Agreement(s).

8.20 **"Underlying Agreement"** means that Agreement under which Business Associate provides a Service to Covered Entity that require the use of PHI or Unsecured PHI. Each Service provided by Cotiviti to Covered Entity is provided under a separate Underlying Agreement for purposes of this BAA, notwithstanding the fact that multiple Services may be purchased under a single Master Software Licensing Agreement or similar master agreement.

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

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