



BUSINESS ASSOCIATE ADDENDUM FOR VENDORS PROVIDING GOODS OR SERVICES TO COTIVITI

This Business Associate Addendum (“BAA”) is by and between Cotiviti, Inc., a Delaware corporation, on behalf of itself and its affiliates (together, “**Cotiviti**”) and any vendor which has contracted to provide goods and services to Cotiviti (“Sub-Business Associate”) and is effective as of the effective date of the Underlying Agreement and is applicable only to the extent set forth in the Recitals.

RECITALS

WHEREAS, Cotiviti is in the business of providing software and licenses for the use of software to customers who make available, transfer and/or disclose confidential, individually identifiable health information (“PHI”) to Cotiviti for the purpose of providing such software services;

WHEREAS, such customers providing PHI to Cotiviti are deemed “Covered Entities” under the definitions of the HIPAA Rules;

WHEREAS, Cotiviti may make available, disclose and/or transfer to Sub-Business Associate its Covered Entities’ PHI during the Parties’ course of performance under the Underlying Agreement;

WHEREAS, in the event that Cotiviti does, in fact, make available, transfer and/or disclose PHI to Sub-Business Associate during the course of the performance of the Underlying Agreement, the Parties recognize that the HIPAA Rules require the Parties bind themselves to a Business Associate Agreement;

WHEREAS, the Parties desire to bind themselves to this Business Associate Addendum and incorporate it into the Underlying Agreement, recognizing that the terms of this Addendum shall apply only when: (1) Cotiviti does, in fact, make available, transfer and/or PHI to Sub-Business Associate during the course of the performance of the Underlying Agreement; and (2) only when the Parties have not entered into another Business Associate Agreement (in which case, the terms of the other BAA control); and

WHEREAS, to the extent that this Addendum is applicable, the Parties agree to comply with applicable regulations governing the use and disclosure of individually identifiable health information, 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. Definitions.

1.1 The terms “Protected Health Information” and “Electronic Protected Health Information” have the meanings set out in 45 C.F.R. § 160.103, limited to the information created or received by Sub-Business Associate from or on behalf of Cotiviti. Protected Health Information may also be referred to as “PHI” or “ePHI”.

1.2 “Effective Date” means the effective date of the Underlying Agreement.

1.3 “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

1.4 “Party” or “Parties” shall mean Cotiviti, Sub-Business Associate, or both, as the context may require.

1.5 “Term” shall mean the term of the Underlying Agreement, including any extensions (whether in whole or in part) to the term of the Underlying Agreement.

1.6 “Underlying Agreement” means the agreement under which Sub-Business Associate provides goods and/or services to Cotiviti.

1.7 Other capitalized terms used but not defined herein shall have the respective meanings given to such terms in the Privacy Rule or Security Rule.

2. Permitted Uses and Disclosures by Sub-Business Associate

2.1 Sub-Business Associate may use or disclose PHI only as necessary to perform the services requested by the Cotiviti or its agent under the Underlying Agreement(s).

2.2 Sub-Business Associate may disclose PHI if Required by Law.

2.3 Sub-Business Associate may use protected health information for the proper management and administration of the Sub-Business Associate or to carry out the legal responsibilities of the Sub-Business Associate.

2.4 Sub-Business Associate may disclose protected health information for the proper management and administration of Sub-Business Associate or to carry out the legal responsibilities of the Sub-Business Associate, provided the disclosures are required by law, or Sub-Business Associate obtains reasonable assurances in writing from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Sub-Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3. Obligations of Sub-Business Associate

3.1 Sub-Business Associate agrees not to use or disclose the PHI other than as expressly permitted or required by this BAA or as Required by Law.

3.2 Sub-Business Associate will make reasonable efforts to use, disclose and request of Cotiviti only the minimum amount of PHI that is reasonably necessary to accomplish the intended purpose of the use, disclosure or request.

3.3 Sub-Business Associate agrees to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to Electronic Protected Health Information, to prevent use or disclosure of PHI other than as provided for by the BAA.

3.4 In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, require that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Sub-Business Associate agree to the same restrictions, conditions, and requirements that apply to the Sub-Business Associate under this BAA with respect to such information, including any encryption requirements.

3.5 To the extent that Sub-Business Associate is to carry out an obligation of Cotiviti under the HIPAA Privacy Rule, Sub-Business Associate agrees to comply with the requirements of the Privacy Rule that would apply to Cotiviti in the performance of such obligation.

3.6 Sub-Business Associate shall not store, transmit or deliver to Cotiviti any PHI in an unencrypted state without Cotiviti’s knowledge and express written consent. Sub-Business Associate 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. Obligations of Cotiviti

4.1 Cotiviti shall notify Sub-Business Associate of any limitations in the Notice of Privacy Practices of its Covered Entity to the extent that such limitations affect Sub-Business Associate's use or disclosure of PHI.

4.2 Cotiviti shall notify Sub-Business Associate of any changes in, or revocation of, permission by an Individual regarding the use or disclosure of PHI, to the extent that such changes may affect Sub-Business Associate's use or disclosure of Protected Health Information.

4.3 Cotiviti agrees to only disclose the minimum amount of PHI to Sub-Business Associate if and to the extent necessary for Sub-Business Associate to provide services under the Underlying Agreement(s) and in compliance with applicable law, and to limit disclosure to the minimum number of personnel for the minimum amount of time necessary for Sub-Business Associate to accomplish the intended purpose of such use, disclosure, or request, respectively.

4.4 Cotiviti shall notify Sub-Business Associate of any restriction on the use or disclosure of PHI that Cotiviti has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Sub-Business Associate's use or disclosure of PHI.

4.5 Cotiviti shall not request Sub-Business Associate to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Cotiviti.

5. Individual Rights

5.1 Sub-Business Associate will, within ten (10) business days following Cotiviti's request, make available to Cotiviti any requested PHI in a Designated Record Set as necessary to satisfy Cotiviti's obligations to its Covered Entity under 45 CFR 164.524 to the extent that Cotiviti does not already have such PHI in its possession, custody or control.

5.2 Sub-Business Associate will, within ten (10) business days following written notice from Cotiviti, promptly amend any portion of the Protected Health Information of Cotiviti's Covered Entity, as necessary so that Cotiviti may meet its amendment obligations under 45 C.F.R. § 164.526.

5.3 To the extent Sub-Business Associate maintains any PHI, it will make available the information required to provide an accounting of disclosures to the Cotiviti as necessary to satisfy Cotiviti's obligations to an Individual under 45 CFR 164.528.

5.4 If requested by the Secretary, Sub-Business Associate will make its internal practices, books, and records available to the Secretary for purposes of determining compliance with applicable regulations.

6. Breach Notification

6.1 Sub-Business Associate agrees to report to Cotiviti any use or disclosure of Protected Health Information not provided for by this BAA of which it becomes aware, including breaches of Unsecured PHI as required at 45 CFR 164.410, and any Security Incident of which it becomes aware that directly affects the PHI.

6.2 Sub-Business Associate will report any Breach of Unsecured PHI to Cotiviti within 24 hours and will provide all relevant information reasonably requested by Cotiviti concerning the details of such Breach, including all measures taken to prevent any further Breach of Unsecured PHI.

6.3 Sub-Business Associate will mitigate, to the extent practicable, any harmful effect of a use or disclosure of PHI not permitted by this BAA, the HIPAA Privacy Rule, or by any other applicable state or federal law or regulation.

6.4 For avoidance of doubt, this section constitutes notice by Sub-Business Associate to Cotiviti 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 Sub-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.

7. Indemnification

7.1. Indemnification Obligation. Unless otherwise addressed in Vendor Agreement, Sub-Business Associate shall defend, indemnify and hold harmless Business Associate, its affiliates and their respective directors, officers and employees from and against all claims, causes of action, damages and expenses (including reasonable attorneys' fees and costs of mitigation measures described in Section 6 arising out of or relating to any Incident or breach of this BAA by Sub-Business Associate and its subcontractors and affiliates. The exclusions and limits of liability, if any, provided in the Underlying Agreement(s) shall not apply to damages arising from a breach of the foregoing obligations.

7.2 Survival. The obligations of Sub-Business Associate under this Section shall survive the termination of this BAA.

8. Term and Termination

8.1. Termination for Cause. If either Party has breached a material term of this BAA that has not been cured within thirty (30) days of the other Party providing notice of such breach, the non-breaching Party may terminate the BAA and the Underlying Agreement(s). In the event that Cotiviti terminates this BAA and the Underlying Agreement(s) for cause pursuant to this Section 8.1, Cotiviti will have no further liability under the Underlying Agreement(s) to Sub-Business Associate.

8.2. Obligations of Sub-Business Associate Upon Termination. Upon termination of this BAA or the Underlying Agreement(s) for any reason, Sub-Business Associate, with respect to PHI received from Cotiviti, or created, maintained, or received by Sub-Business Associate on behalf of Cotiviti, shall:

- 8.2.1. Retain only that Protected Health Information which is necessary for Sub-Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
- 8.2.2. Destroy or return to Cotiviti the remaining Protected Health Information that the Sub-Business Associate still maintains in any form;
- 8.2.3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic Protected Health Information to prevent use or disclosure of the Protected Health Information, other than as provided for in this Section, for as long as Sub-Business Associate retains the Protected Health Information;
- 8.2.4. Not use or disclose the Protected Health Information retained by Sub-Business Associate other than for the purposes for which such Protected Health Information was retained and subject to the same restrictions which applied prior to termination under this BAA; and

8.2.5. Destroy or return to Cotiviti the Protected Health Information retained by Sub-Business Associate when it is no longer needed by Sub-Business Associate for its proper management and administration or to carry out its legal responsibilities.

8.2.6. In the event that Sub-Business Associate determines that returning or destroying the Protected Health Information is commercially unreasonable (e.g., when stored on backup tape), Sub-Business Associate shall provide to Cotiviti notification of the conditions that make return or destruction commercially unreasonable. If that is the case, obligations pursuant to this BAA shall survive for so long as Sub-Business Associate maintains such Protected Health Information.

8.3. Survival. The obligations of Sub-Business Associate under this Section shall survive the termination of this BAA.

9. Miscellaneous

9.1 Regulatory References. A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended.

9.2 Amendment. The Parties agree to take such action as is necessary to amend this BAA from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

9.3 Interpretation. Any ambiguity in this BAA shall be interpreted to permit compliance with the HIPAA Rules.

9.4 No Third-Party Beneficiaries. No third-parties are intended to benefit from this BAA and no third-party beneficiary rights will be implied from anything contained in this BAA.

9.5 Independent Relationship. None of the provisions of this BAA are intended to create, nor will they be deemed to create, any relationship between Cotiviti and Sub-Business Associate other than that of independent parties contracting with each other as independent contractors solely for the purposes of effecting the provisions of this BAA.

9.6 Successor and Assigns. This BAA will inure to the benefit of and be binding upon the successors and assigns of Cotiviti and Sub-Business Associate. However, this BAA is not assignable by any Party without the prior written consent of the other Party, provided that either Party may assign this BAA to a successor in the event of a change of control by way of sale, merger, acquisition or other transaction.

9.7 Entire Agreement. This BAA, along with the Underlying Agreement, constitutes the entire understanding between the parties on this subject, and supersedes all other written, electronic or oral communications, on this subject. This BAA is governed by the Underlying Agreement except to the extent terms in this BAA conflict with the Underlying Agreement, in which case this BAA will govern. This BAA may not be modified or amended except by a written agreement signed by the parties. Any purchase order used by the parties is for administrative use only and any terms included on or referenced by the purchase order are invalid to the extent such terms attempt to modify or supersede the terms of this BAA.