



INNOVATIONS IN
PRODUCTIVITY

BUSINESS ASSOCIATE AGREEMENT

NVOQ INCORPORATED

This Business Associate Agreement (the "Agreement") is made effective as of the effective date of the Software Subscription License Agreement or other alternate agreement between you and nVoq Incorporated whereby PHI may be shared and treated as Confidential Information (the "Effective Date"), by and between Licensee (hereinafter referred to as "Covered Entity") and nVoq Incorporated (hereinafter referred to as "Business Associate") (Covered Entity and Business Associate are hereinafter referred to individually as a "Party" and collectively as the "Parties").

WITNESSETH:

WHEREAS, pursuant to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the U.S. Department of Health & Human Services ("HHS") promulgated the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Standards"), at 45 C.F.R. Parts 160 and 164, requiring certain individuals and entities subject to the Privacy Standards to protect the privacy of certain individually identifiable health information ("Protected Health Information" or "PHI"); and

WHEREAS, the Parties wish to enter into a Business Associate Agreement to ensure compliance with the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA Privacy and Security Rules") (45 C.F.R. Parts 160 and 164); and

WHEREAS, the Health Information Technology for Economic and Clinical Health ("HITECH") Act enacted under the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, modified the HIPAA Privacy and Security Rules and imposed certain privacy and security obligations in addition to the obligations created by the HIPAA Privacy and Security Rules") (hereinafter, all references to the "HIPAA Privacy and Security Rules" include all amendments thereto set forth in the HITECH Act and any accompanying regulations); and

WHEREAS, the Parties have entered into or are entering into a written or oral arrangement or arrangements (the "Prime Contracts") whereby Business Associate will provide certain services to Covered Entity and, pursuant to such Prime Contracts, Business Associate may be considered a "business associate" of Covered Entity as defined in the HIPAA Privacy and Security Rules; and

WHEREAS, Business Associate may have access to Protected Health Information or Electronic Protected Health Information (as defined below) in fulfilling its responsibilities under the Prime Contracts; and

WHEREAS, Covered Entity wishes to comply with the HIPAA Privacy and Security Rules, and Business Associate wishes to honor its obligations as a Business Associate to Covered Entity; and

NOW, THEREFORE, in consideration of the Parties' continuing obligations under the Prime Contracts, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the provisions of this Agreement.

1. DEFINITIONS

1.1 Except as otherwise defined herein, any and all capitalized terms in this Agreement shall have the definitions set forth in the HIPAA Privacy and Security Rules. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the HIPAA Privacy and Security Rules, as amended, the HIPAA Privacy and Security Rules in effect at the time shall control. Where provisions of this Agreement are different than those mandated by the HIPAA Privacy and Security Rules, but are nonetheless permitted by the HIPAA Privacy and Security Rules, the provisions of this Agreement shall control.

1.2 The term "Breach" means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where, to the extent the disclosure would not be treated as a breach under applicable law, an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. The term "Breach" does **not** include: (1) any unintentional acquisition, access, or use of protected health information by any employee or individual acting under the authority of a covered entity or business associate if (a) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate, and (b) such information is not further acquired, accessed, used, or disclosed by any person; or (2) any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; and (3) any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person. Breach also does not include any disclosure that would not otherwise be treated as a breach under applicable law

1.3 The term "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity. "Protected Health Information" includes, without limitation, "Electronic Protected Health Information," as defined below.

1.4 The term “Electronic Protected Health Information” shall have the meaning given to such term under the HIPAA Privacy and Security Rules, including but not limited to 45 C.F.R. Parts 160, 162, and 164, and under HITECH.

1.5 The term “Secretary” means the Secretary of the Department of Health and Human Services (“HHS”) or his or her designee.

1.6 The term “Unsecured Protected Health Information” means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance published in the Federal Register at 74 Fed. Reg. 19006 on April 27, 2009 and in annual guidance published thereafter.

2. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

2.1 Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Prime Contracts, provided that such use or disclosure would not violate the HIPAA Privacy and Security Rules if done by Covered Entity. Until such time as the Secretary issues regulations pursuant to the HITECH Act specifying what constitutes “minimum necessary” for purposes of the HIPAA Privacy and Security Rules, Business Associate shall, to the extent practicable, disclose only Protected Health Information that is contained in a limited data set (as defined in Section 164.514(e)(2) of the HIPAA Privacy and Security Rules), unless the person or entity to whom Business Associate is making the disclosure requires certain direct identifiers in order to accomplish the intended purpose of the disclosure, in which event Business Associate may disclose only the minimum necessary amount of Protected Health Information to accomplish the intended purpose of the use, disclosure, or request for use or disclosure, in accordance with the requirements of HIPAA. Covered Entity shall determine what quantum of information constitutes the “minimum necessary” amount for Business Associate to accomplish its intended purposes.

2.2 Business Associate may not use or disclose Protected Health Information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity, except for the specific uses and disclosures set forth below.

2.3 Business Associate may use Protected Health Information in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of Business Associate, provided that such uses are permitted under state and federal confidentiality laws. Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR 164.504(e)(2)(i)(B).

2.4 Business Associate may disclose Protected Health Information in its possession to third parties with whom it contracts for the purposes of its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that:

2.4.1 The disclosures are required by law; or

2.4.2 Business Associate obtains reasonable assurances from the third parties to whom the Protected Health Information is disclosed that the information will remain confidential and be used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party, and that such third parties will notify Business Associate of any instances of which they are aware in which the confidentiality of the information has been breached.

2.4.3 Without limiting the foregoing, if Business Associate discloses PHI to a “Subcontractor” as defined under the HIPAA Privacy and Security Rules, Business Associate shall execute a Business Associate Agreement with such Subcontractor containing substantially the same terms and conditions as set forth in this Agreement.

2.5 Business Associate shall train the members of its workforce whose function involves contact with PHI to appropriately handle and safeguard PHI. Such training shall, at a minimum, include: implementation and use of risk assessment criteria to determine when a Breach occurs, and how to report a Breach.

3. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

3.1 Business Associate acknowledges and agrees that all Protected Health Information that is created or received by Covered Entity and disclosed or made available in any form, including paper record, oral communication, audio recording, and electronic display by Covered Entity or its operating units to Business Associate or is created or received by Business Associate on Covered Entity’s behalf shall be subject to this Agreement.

3.2 Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by this Agreement or as required by law.

3.3 Business Associate agrees to use appropriate safeguards to prevent use or disclosure of Protected Health Information other than as provided for by this Agreement. Specifically, Business Associate will implement the administrative, physical, and technical safeguards set forth in Sections 164.308, 164.310, and 164.312 (as may be amended from time to time) of the HIPAA Privacy and Security Rules that reasonably and appropriately protect the confidentiality, integrity, and availability of any Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity, and, in accordance with Section 164.316 of the HIPAA Privacy and Security Rules, implement and maintain reasonable and appropriate policies and procedures to enable it to comply with the requirements outlined in Sections 164.308, 164.310, and 164.312; and

3.4 Business Associate agrees to report to Covered Entity the use or disclosure of Protected Health Information not provided for by this Agreement, including breaches of unsecured protected health information as required at 45 CFR 164.410. Further, Business Associate agrees to report to Covered Entity within five (5) days of discovery of any Security Incident of which it Discovers as required by 45 CFR 164.314 For purposes of this Agreement, “Security Incident” means the successful unauthorized access, use, disclosure, modification, or destruction of Protected Health Information or interference with system operations in an information system, of which Business Associate has knowledge or should, with the exercise of reasonable diligence, have knowledge, excluding (i) “pings” on an information system firewall; (ii) port scans; (iii) attempts to log on to an information system or enter a database with an invalid password or user name; (iv) denial-of-service attacks that do not result in a server being taken offline; or (v) malware (e.g., a worms or a virus) that does not result in unauthorized access, use, disclosure, modification or destruction of Protected Health Information.

3.5 Business Associate agrees to ensure that any agent, including, without limitation, any affiliate of Business Associate or any contractor or subcontractor of Business Associate, to whom it provides electronic Protected Health Information or Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions, requirements, and conditions that apply through this Agreement to Business Associate with respect to such information.

3.6 On and after the Effective Date, Business Associate shall comply with any agreement that Covered Entity makes that restricts use or disclosure of Covered Entity's PHI pursuant to 45 C.F.R. § 164.522(a), provided that Covered Entity notifies Business Associate in writing of the restriction or confidential communication. Covered Entity shall promptly notify Business Associate in writing of the termination of any such restriction agreement and, with respect to termination of any such restriction agreement, instruct Business Associate whether any of Covered Entity's PHI will remain subject to the terms of the restriction agreement.

3.7 At the request of Covered Entity and in a reasonable time and manner, Business Associate agrees to make available Protected Health Information required for Covered Entity to respond to an individual's request for access to his or her Protected Health Information in accordance with Section 164.524 of the HIPAA Privacy and Security Rules. If Business Associate maintains Protected Health Information electronically, it agrees to make such Protected Health Information available electronically to the applicable individual or to a person or entity specifically designated by such individual, upon such individual's request.

3.8 At the request of Covered Entity and in a reasonable time and manner, Business Associate agrees to make available Protected Health Information required for amendment by Covered Entity in accordance with the requirements of Section 164.526 of the HIPAA Privacy and Security Rules, or take other measures as necessary to satisfy covered entity's obligations under Section 164.526 of the HIPAA Privacy and Security Rules.

3.9 Business Associate agrees to document any disclosures of and make Protected Health Information available for purposes of accounting of disclosures, as required by Section 164.528 of the HIPAA Privacy and Security Rules.

3.10 Business Associate agrees that it will make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity, available to the Secretary for the purpose of determining Covered Entity's compliance with the HIPAA Privacy and Security Rules, in a time and manner designated by the Secretary.

3.11 Business Associate agrees that, while present at any Covered Entity facility and/or when accessing Covered Entity's computer network(s), it and all of its employees, agents, representatives and subcontractors will at all times comply with any network access and other security practices, procedures and/or policies established by Covered Entity including, without limitation, those established pursuant to the HIPAA Privacy and Security Rules.

3.12 On and after the Effective Date, Business Associate agrees that it will not directly or indirectly receive remuneration for any written communication that encourages an individual to purchase or use a product or service without first obtaining the written authorization of the individual or the individual's representative, unless the communication is made on behalf of Covered Entity and is consistent with the terms of this Agreement.

3.13 On and after the Effective Date, Business Associate agrees that if it uses or discloses patients' Protected Health Information for marketing purposes, it will obtain such patients' authorization before making any such use or disclosure.

4. BUSINESS ASSOCIATE'S MITIGATION AND BREACH NOTIFICATION OBLIGATIONS

4.1 Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

4.2 Following the discovery of a Breach of Unsecured Protected Health Information, Business Associate shall notify Covered Entity of such Breach without unreasonable delay and in no case later than 24 hours after discovery of the Breach. A Breach shall be treated as discovered by Business Associate as of the first day on which such Breach is known to Business Associate or, through the exercise of reasonable diligence, would have been known to Business Associate.

5. OBLIGATIONS OF COVERED ENTITY

5.1 Upon request of Business Associate, Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with Section 164.520 of the HIPAA Privacy and Security Rules.

5.2 Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by an individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.

5.3 Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information to which Covered Entity has agreed in accordance with Section 164.522 of the HIPAA Privacy and Security Rules, and Covered Entity shall inform Business Associate of the termination of any such restriction, and the effect that such termination shall have, if any, upon Business Associate's use and disclosure of such Protected Health Information.

5.4 Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the HIPAA Privacy and Security Rules if done by Covered Entity

6. TERM AND TERMINATION

6.1 Term. The Term of this Agreement shall be effective as of the Effective Date, and shall terminate upon the later of the following events: (i) in accordance with Section VII(c), when all of the Protected Health Information 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 or, if such return or destruction is infeasible, when protections are extended to such information; or (ii) upon the expiration or termination of the last of the Prime Contracts.

6.2 Termination for Cause. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall have the right to immediately terminate this Agreement and the Prime Contracts. If termination is not feasible, Covered Entity shall report such violation to the Secretary.

6.3 Effect of Termination. Except as provided in paragraph 7.3.1 of this subsection, upon termination of this Agreement, the Prime Contracts or upon request of Covered Entity, whichever occurs first, Business Associate shall within ten (10) days return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Neither Business Associate nor its subcontractors or agents shall retain copies of the Protected Health Information.

6.3.1 In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide within ten (10) days to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

7. MISCELLANEOUS

7.1 A reference in this Agreement to a section in the HIPAA Privacy and Security Rules means the section as in effect or as amended. In the event that a regulatory citation contained within this Agreement should change prior to this Agreement being amended, the regulatory citation in this Addendum shall be deemed to have been changed to the new citation.

7.2 No Rights in Third Parties. Except as expressly stated herein or in the HIPAA Privacy and Security Rules, the Parties to this Agreement do not intend to create any rights in any third parties.

7.3 Survival. The obligations of Business Associate under Section VII(c) of this Agreement shall survive the expiration, termination, or cancellation of this Agreement, the Prime Contracts, and/or the business relationship of the parties, and shall continue to bind Business Associate, its agents, employees, contractors, successors, and assigns as set forth herein.

7.4 Amendment. This Agreement may be amended or modified only in a writing signed by the Parties. The Parties agree that they will negotiate amendments to this Agreement to conform to any changes in the HIPAA Privacy and Security Rules as are necessary for Covered Entity to comply with the current requirements of the HIPAA Privacy and Security Rules or the Health Insurance Portability and Accountability Act. In addition, in the event that either Party believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the HIPAA Privacy and Security Rules or any other applicable legislation, then such Party shall notify the other Party of its belief in writing. For a period of up to thirty (30) days, the Parties shall address in good faith such concern and amend the terms of this Agreement, if necessary to bring it into compliance. If, after such thirty (30)-day period, the Agreement fails to comply with the HIPAA Privacy and Security Rules or any other applicable legislation, then either Party has the right to terminate this Agreement and the Prime Contracts upon written notice to the other party.

7.5 Assignment. Except as otherwise expressly permitted under this Agreement, neither party may assign or transfer, by operation of law or otherwise, any of its rights under this Agreement or delegate any of its duties under this Agreement to any third party without the other party's prior written consent, not to be unreasonably withheld; provided, however, each party may assign, in whole or in part, its rights and obligations hereunder to (a) a successor legal entity resulting from a merger, consolidation, or non-bankruptcy consolidation or to a purchaser of all or substantially all of said party's assets or a majority, or controlling interest in said party's voting stock, provided that the purchaser's net worth at the time of purchase is equal to or greater than that of said party; or (b) a present or future subsidiary or affiliate of said party. Any attempted assignment or transfer in violation of the foregoing will be void and of no force and effect. Subject to the foregoing, this Agreement will be binding upon, and will inure to the benefit of, the parties and their respective successors and permitted assigns.

7.6 Independent Contractor. None of the provisions of this Agreement are intended to create, nor will they be deemed to create, any relationship between the Parties other than that of independent parties contracting with each other solely for the purposes of effecting the provisions of this Agreement and any other Prime Contracts between the Parties evidencing their business relationship.

7.7 Governing Law. To the extent this Agreement is not governed exclusively by the HIPAA Privacy and Security Rules or other provisions of federal statutory or regulatory law, it will be governed by and construed in accordance with the laws of the state of Colorado.

7.8 No Waiver. No change, waiver, or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

7.9 Interpretation. Any ambiguity of this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the HIPAA Privacy and Security Rules.

7.10 Severability. In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect.

7.11 Notice. Any notification required in this Agreement shall be made in writing to the representative of the other Party who signed this Agreement or the person currently serving in that representative's position with the other Party.

7.12 Certain Provisions Not Effective in Certain Circumstances. The provisions of this Agreement relating to the HIPAA Security Rule shall not apply to Business Associate if Business Associate does not receive any Electronic Protected Health Information from or on behalf of Covered Entity.