

EXHIBIT B

BUSINESS ASSOCIATE AND QUALIFIED SERVICE ORGANIZATION AGREEMENT

This Business Associate & Qualified Service Organization Agreement (the “BAA”) is incorporated into the First Amended and Restated Risk-Bearing Participant & Preferred Provider Agreement (the “Agreement”) entered into by and between **OneCare Vermont Accountable Care Organization, LLC** (“Business Associate”) and <xcd_contract_desc> (“Covered Entity”).

RECITALS

Covered Entity and Business Associate are parties to the Agreement pursuant to which Business Associate provides certain services to Covered Entity and, in connection with those services, Covered Entity discloses to Business Associate or permits disclosure to Business Associate certain Protected Health Information (“PHI”) that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and Title XIII, The Health Information Technology for Economic and Clinical Health Act (“HITECH”), of the American Recovery and Reinvestment Act (“ARRA”) and may also be subject to 42 USC § 290dd-2 and 42 CFR Part 2.

Under the terms of the Agreement and for purposes of sharing PHI for population health management purposes, Business Associate and Covered Entity have also agreed to participate in an Organized Health Care Arrangement (“OHCA”) as that term is defined under HIPAA and the Agreement.

The parties desire to comply with the requirements set forth in the Privacy and Security Regulations and HITECH concerning the privacy of PHI.

The purpose of this Addendum is to comply with the requirements of the Privacy Rule, the Security Rule, HITECH and, if applicable, 42 CFR Part 2 including but not limited to the Business Associate Requirements at 45 C.F.R. Section 164.504(e) and the Qualified Service Organization provisions at 42 CFR Sections 2.11 and 2.12(c)(4).

Therefore, in consideration of the mutual promises and covenants contained herein, the parties agree as follows:

SECTION I – DEFINITIONS

- 1.1 **Definitions.** Unless otherwise provided in this BAA, capitalized terms shall have the same meaning as set forth in the HIPAA regulations, 45 C.F.R. Sections 160 and 164, and HITECH and its related regulations or under 42 CFR Section 2.11.

SECTION II – OBLIGATIONS OF BUSINESS ASSOCIATE

- 2.1 Use/Disclosure of PHI. In connection with its use and disclosure of PHI, Business Associate agrees that it shall use and/or disclose PHI only as permitted or required by this BAA or as otherwise required by law.
- 2.2 Safeguards for Protection of PHI. Business Associate agrees to use reasonable and appropriate safeguards to prevent the use or disclosure of PHI other than as provided in this BAA.
- 2.3 Compliance with HITECH Act and Regulations. Business Associate will comply with the requirements of HITECH, codified at 42 U.S.C. §§ 17921-17954, which are applicable to Business Associate, and will comply with all regulations issued by the Department of Health and Human Services to implement these referenced statutes, as of the date by which Business Associate is required to comply with such referenced statutes and HHS regulations.
- 2.4 General Reporting. Business Associate shall report to Covered Entity any use or disclosure of PHI which is not provided for by this BAA of which Business Associate becomes aware.
- 2.5 Reporting of Breaches of Unsecured Protected Health Information. Business Associate will report in writing to Covered Entity's Privacy Officer any Breach of Unsecured PHI, as defined in the Breach Notification Regulations, within ten (10) business days of the date Business Associate learns of the incident giving rise to the Breach. Business Associate will provide such information to Covered Entity as required in the Breach Notification Regulations. Business Associate will reimburse Covered Entity for any reasonable expenses Covered Entity incurs in notifying Individuals of a Breach caused by Business Associate or Business Associate's subcontractors or agents, and for reasonable expenses Covered Entity incurs in mitigating harm to those Individuals. Business Associate also will defend, hold harmless and indemnify Covered Entity and its employees, agents, officers, directors, members, contractors, and subsidiary and affiliate entities, from and against any claims, losses, damages, liabilities, costs, expenses, penalties or obligations (including attorneys' fees) which Covered Entity may incur due to a Breach caused by Business Associate or Business Associate's subcontractors or agents.
- 2.6 Mitigation. Business Associate shall make reasonable efforts to mitigate, to the greatest extent possible, any harmful effects arising from any improper use and/or disclosure of PHI.
- 2.7 Subcontractors. Business Associate shall ensure that any agents, including any ACO Other Entities or subcontractors, to whom it provides PHI, shall agree to the same restrictions and conditions that apply to Business Associate with respect to PHI.

- 2.8 Access by Individuals. Business Associate shall allow individuals who are the subject of the PHI to inspect and copy their PHI in the possession of Business Associate if Covered Entity does not also maintain such information.
- 2.9 Access by Department of Health and Human Services. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services for purposes of determining Covered Entity's compliance with the HIPAA privacy regulations.
- 2.10 Access by Covered Entity. Upon reasonable notice, Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI available to Covered Entity for purposes of determining Business Associate's compliance with the terms of this Agreement and Business Associate's compliance with HIPAA and HITECH.
- 2.11 Accountings of Disclosures. If Business Associate discloses any PHI, Business Associate shall make available to Covered Entity the information necessary for Covered Entity to provide an Accounting of Disclosures to any Individual who requests such an Accounting, or, in the alternative, Business Associate shall provide an Accounting of Disclosures directly to the requesting Individual, if requested by Covered Entity.
- 2.12 Amendment of PHI. Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to Covered Entity's obligations under the Privacy Rule.

SECTION III – PERMITTED USES AND DISCLOSURES

- 3.1 General. Except as otherwise limited in this BAA, Business Associate may use or disclose PHI to perform ACO Activities or on behalf of, Covered Entity as specified in the Agreement and allowed by an OHCA, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity.

SECTION IV – OBLIGATIONS OF COVERED ENTITY

- 4.1 Notice of Privacy Practices. Covered Entity has included and will continue to include, in the Covered Entity Notice of Privacy Practices information advising Individuals that Covered Entity may disclose their PHI to Business Associates.
- 4.2 Consents/Authorizations. Covered Entity has obtained and will continue to obtain, from Individuals, consents, authorizations and other permissions that may be required by the Privacy Rule or applicable state laws and/or regulations prior to furnishing Business Associate PHI pertaining to Individuals.

- 4.3 Restrictions. Covered Entity will promptly notify Business Associate in writing of any restrictions on the use and disclosure of PHI about Individuals that Covered Entity has agreed to that may affect Business Associate's ability to perform its obligations under the Agreement or this BAA.
- 4.4 Revocation of Authorization. Covered Entity shall promptly notify Business Associate in writing of any change in, or revocation of, permission by an Individual to use or disclose PHI, if such changes or revocation may affect Business Associate's ability to perform its obligations under the Agreement or this BAA.

SECTION V – SECURITY

- 5.1 Compliance with Security Rule. Business Associate agrees to implement the Security Rule (security standards as set out in 45 C.F.R. parts 160, 162 and 164), Administrative, Physical and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity, and Availability of the electronic PHI that Business Associate creates, receives, maintains, or transmits on behalf of the Covered Entity.
- 5.2 Reporting. Business Associate agrees to report to Covered Entity any security incident of which it becomes aware.
- 5.3 Agents Compliance with Business Associate Addendum. Business Associate agrees to ensure that any agent, including a subcontractor or ACO Other Entity, to whom it provides PHI received from, or created or received by, Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this BAA to Business Associate with respect to such information.
- 5.4 Agents Compliance with Security Rule. Business Associate will ensure that any agent, including a subcontractor or ACO Other Entity, to whom it provides electronic PHI agrees to implement the Security Rule, Administrative, Physical and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity, and Availability of the electronic PHI.
- 5.5 Records Availability. Business Associate agrees to make its policies, procedures, and documentation relating to the safeguards described herein available to the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Security Rule.

SECTION VI – TERM & TERMINATION

- 6.1 Term and Termination. This BAA shall be effective as of effective date of the Agreement and shall terminate when 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. The parties acknowledge and agree

that the terms and conditions stipulated in this BAA shall apply to any future written or oral agreements between Covered Entity and Business Associate which require the disclosure of PHI, whether or not this BAA is incorporated by reference into future agreements executed between the parties. This BAA shall terminate in accordance with the termination provisions in the Agreement.

- 6.2 Effect of Termination. Upon termination of the Agreement, for any reason, Business Associate shall, if feasible, return or destroy all PHI that Business Associate still maintains in any form and shall not retain any copies of such PHI. If such return or destruction is not feasible, Business Associate shall extend the protections of this Agreement to the PHI and shall limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible. Notwithstanding the foregoing, Covered Entity acknowledges that Business Associate receives some PHI, with Covered Entity's consent, from third-party payers that may not be able to be returned or destroyed on behalf of Covered Entity. In the event Business Associate must maintain PHI after termination it will continue to protect such PHI in accordance with HIPAA for the time that it possesses the PHI. Nothing in this BAA shall prohibit the Business Associate from de-identifying PHI, in accordance with HIPAA, and using such de-identified information for ACO Activities during the term of or after the Agreement has terminated.

SECTION VII – QUALIFIED SERVICE ORGANIZATION PROVISIONS

- 7.1 Applicability. This Section shall only apply in the event that Business Associate is also considered a Qualified Services Organization, as defined in 42 CFR § 2.11, because the Covered Entity or Covered Entity Affiliate is subject to 42 CFR Part 2 ("Part 2 Program").
- 7.2 Limits on Use and Disclosure. Where Business Associate acts as a Qualified Services Organization it agrees to the following limits on use and disclosure:
- a. Business Associate shall only access Part 2 Program information to the extent needed by it to provide the services described in this Agreement.
 - b. Business Associate agrees not to use or further disclose any Part 2 Program information other than as specified in this Agreement.
 - c. Business Associate acknowledges that in receiving, storing, processing, or otherwise using any PHI from a Part 2 Program, it is fully bound by the provisions of the federal regulations governing confidentiality of alcohol and drug abuse treatment records, 42 CFR Part 2.
 - d. Business Associate undertakes to resist in judicial proceedings any effort to obtain access to PHI pertaining to Part 2 Program patients other than as expressly

provided for in 42 CFR Part 2, and Business Associate shall notify Covered Entity in such case.

SECTION VIII – MISCELLANEOUS

- 8.1 Amendment. This BAA shall be deemed to amend automatically, by force of law and without further act of the parties, if necessary to bring the Agreement into compliance with any changes in HIPAA, HITECH or any related regulations that are made after the date of execution of this Agreement.
- 8.2 Interpretation. Any ambiguity in this BAA shall be resolved in a manner that brings the BAA into compliance with the then most current version of HIPAA and the HIPAA privacy regulations.
- 8.3 No Third Party Beneficiaries. Nothing express or implied in this BAA is intended to confer, nor shall anything herein confer, upon any other person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.