

PARTICIPANT-CONSORTIUM HIPAA BUSINESS ASSOCIATE AGREEMENT

HIPAA BUSINESS ASSOCIATE AGREEMENT

National Rural Accountable Care Consortium

THIS HIPAA BUSINESS ASSOCIATE AGREEMENT (the “Agreement”) is entered into and effective on _____ (the “Effective Date”), by and between National Rural Accountable Care Consortium (“Business Associate”), and _____ (“Subcontractor Business Associate”) (collectively, the “Parties”) in order to comply with federal privacy and security standards promulgated under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), located at 45 C.F.R. parts 160, 162, and 164, Subpart C, as amended from time to time by the Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH”) and the Final Omnibus Rule (collectively “HIPAA”).

WHEREAS, Subcontractor Business Associate performs functions or activities on behalf of Business Associate involving the creation, receipt, maintenance, or transmission of protected health information (“PHI”) and electronic PHI, including but not limited to, data aggregation, management, administrative, and/or financial services on behalf of Business Associate;

WHEREAS, Subcontractor Business Associate will receive CMS Records from Business Associate and must abide by applicable restrictions in the attached CMS DUA;

WHEREAS, Business Associate may disclose PHI to Subcontractor Business Associate during the course of performance of the above functions or activities;

WHEREAS, Subcontractor Business Associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of PHI that are not authorized by the Services Agreement or this Agreement or required by law, and for failing to safeguard electronic PHI in accordance with the HIPAA Security Rule; and

WHEREAS, The Parties acknowledge their respective obligations to protect the privacy and provide for the security of PHI in compliance with HIPAA.

NOW THEREFORE, for purposes of compliance with HIPAA, the Parties agree to the terms and conditions set forth in this Agreement:

- 1. Definitions.** Terms used, but not otherwise defined, in this Agreement shall have the meaning given by 45 C.F.R. parts 160 and 164. If a term defined herein conflicts with the definition given in 45 C.F.R. parts 160 and 164, the regulatory definition shall prevail.

“Designated Record Set” means a group of records maintained by or for a covered entity. The term “record” means any item, collection, or grouping of information that includes PHI and is created, maintained, collected, used, or disseminated by or for a covered entity.

“CMS Records” means records that originate at CMS and are described in Section 5 of the attached CMS DUA.

2. **Compliance with Applicable Law.** The Parties acknowledge and agree that, beginning with the applicable compliance dates, each party shall comply with its obligations under this Agreement and with all related obligations under HIPAA and other applicable state and federal laws and regulations, as they exist at the time this Agreement is executed and as they are amended or superseded, for so long as this Agreement is in place.
3. **Subcontractor Business Associate use and disclosure of PHI.**

Except as otherwise permitted by this agreement, Subcontractor Business Associate shall not use and disclose PHI unless necessary and appropriate to carry out the purposes specified in this Agreement, the Data Use Agreement between Centers for Medicare and Medicaid Services and ACO (CMS DUA) and for such other purposes as permitted by HIPAA and as required by law. Subcontractor Business Associate will ensure that its directors, officers, employees, subcontractors and agents abide by the restrictions, terms and conditions of this agreement.

Management, Administration, and Legal Uses. Subcontractor Business Associate may use and disclose PHI as necessary for the proper management and administration of Subcontractor Business Associate, or to carry out its legal responsibilities if such use or disclosure is required by law. In these cases, prior to making any such disclosure, Subcontractor Business Associate shall obtain reasonable assurance from the person or entity to whom the PHI is disclosed that: (a) PHI will be held confidential and further used and disclosed only as required by law or for the purpose for which it was disclosed to the person or entity; and (b) the person or entity will notify Subcontractor Business Associate of any instances of which it is aware that confidentiality of the PHI has been breached.

Aggregation. Except as otherwise limited in this Agreement, Subcontractor Business Associate may use PHI to provide Data Aggregation services on behalf of Business Associate, relating to the health care operations of the Covered Entity with whom Business Associate has contracted to perform services, as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

Disclosure to Third Parties. If Subcontractor Business Associate discloses PHI created, maintained, or transmitted by or on behalf of Business Associate to a subcontractor, Subcontractor Business Associate will execute a written agreement with the subcontractor that prohibits the directors, officers, employees, subcontractors and agents of that subcontractor from: (i) using or disclosing PHI in any manner that is not permitted or required by the Services Agreement or this Agreement, or required by law; and (ii) using or disclosing such information in a manner that would violate HIPAA if used or disclosed by Business Associate.

Agreements with Third Parties. Subcontractor Business Associate shall enter into an agreement with any subcontractor that will create, receive, maintain or transmit PHI on behalf of the Subcontractor Business Associate in connection with the services Subcontractor Business Associate provides to or on behalf of Business Associate. Pursuant to such agreement, the agent or subcontractor shall agree to be bound by the same restrictions, terms, and conditions that apply to Subcontractor Business Associate with respect to such PHI, including, without limitation, the breach notification requirements set forth in 45 C.F.R. § 164.410.

Minimum Necessary. All uses and disclosures of and requests by Subcontractor Business Associate for PHI are subject to the minimum necessary rule of HIPAA as specified in 45 C.F.R. § 164.514(d), as applicable.

De-identified Information. Subcontractor Business Associate may use and disclose de-identified health information if the de-identification is in compliance with 45 C.F.R. §164.502(d), and the de-identified health information meets the standard and implementation specifications for de-identification under 45 C.F.R. §164.514(a) and (b).

Withdrawal of Authorization. If the use or disclosure of PHI in this Agreement is based on an individual's specific authorization for the use or disclosure of his or her PHI, and that individual revokes such authorization, or the authorization is invalid or has expired, Subcontractor Business Associate shall, upon notice of such revocation, expiration or invalidation, stop the use or disclosure of the individual's PHI, unless an exception under the HIPAA rules expressly applies.

CMS RECORD REQUIREMENTS

Cell Size Suppression. Subcontractor Business Associate agrees that any use of CMS Records described in the CMS DUA (attached) in the creation of any document (manuscript, table, chart, study, report, etc.) concerning the purpose specified in section 4 of the CMS DUA must adhere to CMS' current cell size suppression policy. This policy stipulates that no cell (e.g. admittances, discharges, patients, services) 10 or less may be displayed. Also, no use of percentages or other mathematical formulas may be used if they result in the display of a cell 10 or less.

Linking Records. Subcontractor Business Associate agrees that, absent express written authorization from Business Associate, the Subcontractor Business Associate shall not attempt to link CMS Records to any other individually identifiable source of information. This includes attempts to link the data to other CMS data file(s).

Reuse. Subcontractor Business Associate understands and agrees that they may not reuse original or derivative data file(s) without prior written approval from Business Associate.

4. **Business Associate use and disclosure of PHI.** In connection with the services provided by Subcontractor Business Associate to or on behalf of Business Associate described this agreement, Business Associate may disclose PHI to Subcontractor Business Associate for the purposes contemplated by the Services Agreement or this agreement.

5. **Required Safeguards To Protect PHI.** Subcontractor Business Associate agrees that it will implement and maintain appropriate safeguards to prevent the use or disclosure of PHI other than pursuant to the terms and conditions of the Services Agreement or this Agreement. To the extent that Subcontractor Business Associate accesses, creates, receives, maintains or transmits PHI in performance of its duties on behalf of Business Associate, Subcontractor Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the PHI, as required by 45 C.F.R. §§164.302-164.414. Subcontractor Business Associate shall also ensure that any subcontractor agrees to implement reasonable and appropriate safeguards to protect the confidentiality, integrity and availability of the PHI that it creates, receives, maintains, or transmits on behalf of Subcontractor Business Associate.

PHI Originating at CMS. CMS Records received by Subcontractor Business Associate must be protected according to additional privacy and security standards. The safeguards used by Subcontractor Business Associate for this PHI shall provide a level and scope of security that is not less than the level and scope of security requirements established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems (<http://www.whitehouse.gov/omb/circulars/a130/a130.html>) as well as Federal Information Processing Standard 200 entitled "Minimum Security Requirements for Federal Information and Information Systems" (<http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>); and, Special Publication 800-53 "Recommended Security Controls for Federal Information Systems" (<http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf>). Subcontractor Business Associate acknowledges that the use of unsecured telecommunications, including the Internet, to transmit individually identifiable, bidder identifiable or deducible information derived from CMS files is prohibited.

6. **Reporting to Business Associate.** Subcontractor Business Associate shall report to Business Associate any use or disclosure of PHI not expressly permitted or required by the Services Agreement, this Agreement or required by law, including security incidents and breaches of unsecured PHI in accordance with the breach notification rule at 45 C.F.R. § 164.410. Business Associate is responsible for reporting to Covered Entities within 60 days, so Subcontractor Business Associate will make reasonable efforts to assist ACO Business Associate in meeting such obligation. Notification shall include, to the extent possible, the identification of each individual whose PHI has been, or is reasonably believed by Subcontractor Business Associate to have been, accessed, acquired, used, or disclosed during the breach, and any other information Business Associate requires, which the Subcontractor Business Associate has readily available, to include in the notification to the individual under 45 C.F.R. 164.404(c). If not all of the information is available within such the expected reporting period, Subcontractor Business Associate will provide the information that is available and continue diligent investigation and provide supplemental information as soon as reasonably practical and in no event later than ninety (90) days after becoming aware of the improper use, disclosure or Security Incident. Where Subcontractor Business Associate is responsible for the improper use or disclosure, Subcontractor Business Associate shall cooperate with any related investigation, analysis,

notification and mitigation activities, and shall be responsible for all costs, damages, fees, penalties and related mitigation efforts for those activities in which the Business Associate is required by law or agreement to participate.

7. **Documentation of Security Incidents.** Subcontractor Business Associate agrees to document all Security Incidents and their outcomes.
8. **Mitigation of Harmful Effects.** Subcontractor Business Associate agrees to mitigate, to the extent practicable, any harmful effect of a use or disclosure of PHI by Subcontractor Business Associate in violation of the requirements of HIPAA or this Agreement, including, but not limited to, compliance with any state law or contractual data breach requirements.
9. **Rights of Individuals Regarding Designated Record Sets.** If Subcontractor Business Associate maintains a Designated Record Set for or on behalf of Business Associate, Subcontractor Business Associate agrees to the following:

Access to Information. Subcontractor Business Associate shall timely make PHI requested by an individual available to Business Associate (for so long as such information is maintained in the Designated Record Set), as required by 45 C.F.R. § 164.524. Business Associate is responsible for enabling Covered Entities to provide PHI from the Designated Record Set within 60 days, so Subcontractor Business Associate will make reasonable efforts to assist Business Associate in meeting such obligation. In the event any individual requests access to PHI directly from Subcontractor Business Associate, the Subcontractor Business Associate shall, within two (2) days, forward such request to Business Associate. If Business Associate maintains the Designated Record Set, Business Associate, rather than Subcontractor Business Associate, shall permit access according to its policies and procedures.

Availability of PHI for Amendment. Within ten (10) days of receipt of a request from Business Associate for amendment of an individual's PHI or a record regarding an individual contained in a Designated Record Set (for so long as the PHI is maintained in the Designated Record Set), Subcontractor Business Associate shall provide such information to Business Associate for amendment and incorporate such amendments in the PHI if amendment is appropriate according to 45 C.F.R. § 164.526. In the event an individual makes a request for an amendment directly to Subcontractor Business Associate, such request shall be forwarded to Business Associate within two (2) days.

Accounting of Disclosures. Business Associate is responsible for enabling Covered Entities to provide an accounting of disclosures to an individual within 30 days. Subcontractor Business Associate agrees to document disclosures of PHI and information related to such disclosures as would allow Business Associate to assist Covered Entities to respond to an individual's request for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. At a minimum, Subcontractor Business Associate shall provide Business Associate with the following information within ten (10) days of request by Covered Entity, for each disclosure that occurred during the shorter of the six years prior to the date of the request or the time period specified in the individual's request: (i) the date

of the disclosure; (ii) the name of the entity or person who received the PHI, and if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of such disclosure that includes an explanation of the basis for such disclosure or a written request for disclosure, if applicable. In the event the request for an accounting is delivered directly to Business Associate, such request shall be forwarded to the Covered Entity within two (2) days.

10. **Other Obligations.** To the extent that Subcontractor Business Associate is responsible under the Services Agreement for performing Business Associate's obligations under the Privacy Rule, Subcontractor Business Associate shall comply with the requirements of the Privacy Rule that apply to the Business Associate in the performance of such obligations in accordance with 45 C.F.R. § 164.504(e)(2)(ii)(H).
11. **Qualified Service Organization.** Subcontractor Business Associate acknowledges that it may be a Qualified Service Organization ("QSO"), as defined in 42 CFR § 2.11, with regard to the services provided to Business Associate. Disclosures by Business Associate to a QSO that describe any personally identifiable alcohol or drug abuse diagnosis, treatment, or referral for treatment don't require written consent. However, Subcontractor Business Associate acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with these alcohol and drug abuse patient records, it is fully bound by the provisions of the federal regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records (found at 42 C.F.R. Part 2)("Confidentiality Regulations"). Under these regulations, certain PHI may not be disclosed or re-disclosed without the patient's written consent, even though such disclosure or re-disclosure might be permitted by HIPAA or other laws. Subcontractor Business Associate will also resist in judicial proceedings any efforts to obtain applicable PHI except as permitted by the Confidentiality Regulations.
12. **Availability of Books and Records.** Subcontractor Business Associate agrees to make its internal practices, policies, procedures, books, and records relating to the use and disclosure of PHI, including those received from or on behalf of Business Associate, available to Business Associate, authorized representatives of CMS or DHHS Office of the Inspector General and/or the Secretary according to 45 C.F.R. 160.310(c), for purposes of determining compliance with HIPAA and the CMS DUA.
13. **Breach of Contract by Subcontractor Business Associate; Termination.**
 - (a) In addition to any other rights Business Associate may have under the Services Agreement, this Agreement or by operation of law or in equity, and notwithstanding any provisions in the Services Agreement, Business Associate may: (i) immediately terminate the Services Agreement and this Agreement if Business Associate is aware of a pattern of activity or practice of the Subcontractor Business Associate in violation of HIPAA or this Agreement or if Business Associate determines that Subcontractor Business Associate has violated a material term of this Agreement; or (ii) at Business Associate's option, permit Subcontractor Business Associate to cure or end any such violation within the time specified by Business Associate.

- (b) Business Associate's option to permit Subcontractor Business Associate to cure a breach of this Agreement shall not be construed as a waiver of any other rights Business Associate has in the Services Agreement, this Agreement or by operation of law or in equity.

14. Destruction of Records.

- (a) Upon the termination of the Services Agreement or this Agreement for any reason, Subcontractor Business Associate shall, if feasible, return to Business Associate or destroy all PHI received from Business Associate, or created or received by Subcontractor Business Associate on behalf of Business Associate, that Subcontractor Business Associate maintains in any form, recorded on any medium, or stored in any storage system. Subcontractor Business Associate shall retain no copies of the PHI.
- (b) In the event that Subcontractor Business Associate reasonably determines that returning or destroying the PHI is not feasible, Subcontractor Business Associate shall extend the protections required by HIPAA and this Agreement and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Subcontractor Business Associate maintains such PHI.
- (c) Note: The CMS DUA requires that the Business Associate destroy PHI received from CMS once the term of the CMS DUA ends, the CMS DUA is terminated, or upon request by CMS. To help the Business Associate comply with this requirement, Subcontractor Business Associate shall destroy all files described in the CMS DUA (attached) upon request of the Business Associate.

15. Third Party Rights. The terms of this Agreement are not intended, nor should they be construed, to grant any rights to any parties other than Subcontractor Business Associate and Business Associate.

16. Indemnification. Each party shall be legally and financially responsible for the acts and omissions of itself and its employees, directors, officers, representatives and agents and will pay all losses and damages attributable to such acts or omissions for which it is legally liable. This Agreement shall not be construed to create a contractual obligation for one party to indemnify the other party for loss or damage resulting from any act or omission of such other party or its employees, directors, officers, representatives or agents, nor to constitute a waiver by either party of any rights to indemnification, contribution or subrogation that the party may have by operation of law.

17. No Agency. This Agreement is not intended to create an agency or joint venture arrangement between the Parties.

18. Owner of PHI. Under no circumstances shall Subcontractor Business Associate be deemed in any respect to be the owner of any PHI accessed, created, maintained or transmitted by Subcontractor Business Associate pursuant to the terms of the Services Agreement or this Agreement.

19. Changes in the Law. Upon prior written notice to the other party, either party may amend either the Services Agreement or this Agreement, as appropriate, to the extent necessary to conform to any new or revised legislation, rules and regulations to which either party is subject now or in the future including, without limitation, HIPAA.

20. Judicial and Administrative Proceedings. In the event Subcontractor Business Associate receives a subpoena, court or administrative order or other discovery request or mandate for release of PHI, Subcontractor Business Associate shall notify Business Associate of the request or mandate as soon as reasonably practicable, but in any event within two (2) days of receipt of such request or mandate and prior to responding to any such request or mandate. Business Associate shall have the right and opportunity to object to such request or mandate, and any relevant covered entities may seek a protective order or equivalent to ensure protection of the PHI, any applicable individual privacy rights, and applicable business operations.

21. Conflicts. If there is any direct conflict between the Services Agreement and this Agreement, the terms and conditions of this Agreement shall control.

IN WITNESS WHEREOF, the Parties have executed this Agreement the day and year first above written.

**SUBCONTRACTOR BUSINESS
ASSOCIATE:**

BUSINESS ASSOCIATE:

Signed

Signed

Printed

Printed

Date

Date

Address for notices:

Address for notices:

National Rural Accountable Care Consortium
P.O. Box 1330
Nevada City, CA 95959