

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the “Agreement”) is entered into between **Triple Aim Accountable Care Organization d/b/a Community Health Network (“CHN”)** and _____ (“Business Associate”) as of the dates set forth below. This Agreement replaces any prior business associate agreement entered into between the parties.

WHEREAS, the parties have entered into one or more arrangements (each, an “Arrangement”), including that certain Participation Agreement, whereby, through its activities for or on behalf of CHN, the Business Associate may have access to Individually Identifiable Health Information; and

WHEREAS, the parties agree as follows:

ARTICLE I **Definitions**

1.1 The following terms shall have the following meanings when used in this Agreement:

- A. “Breach” as used in Section 3.14 of this Agreement means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of 45 C.F.R. Part 164 which compromises the security or privacy of the protected health information.
- B. “Breach Notification Standards” means the current federal standards for Notification in the Case of Breach of Unsecured Protected Health Information codified at 45 C.F.R. Part 164, Subpart D and promulgated under Section 13402 of the HITECH Act.
- C. “Compliance Date” means, in each case, the date by which compliance is required under the referenced provision of the HITECH Act and/or its implementing regulations, as applicable; provided that, in any case for which the Compliance Date occurs prior to the date of the applicable Arrangement, the Compliance Date shall mean the date of the applicable Arrangement.
- D. “DHHS” means the United States Department of Health and Human Services.
- E. “Electronic Media” means electronic storage media, on which data is or may be recorded electronically, including computer hard drives, magnetic tapes or disks, optical disks, or digital memory cards, or transmission media used to exchange information already in electronic storage media, including the internet, extranet, leased lines, dial-up lines, private networks, and transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

- F. “Electronic PHI” means PHI that is transmitted by or maintained in Electronic Media.
 - G. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996.
 - H. “HITECH Act” means Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009 and any and all existing and future implementing regulations promulgated under such provisions, when and as each is effective.
 - I. “Individually Identifiable Health Information” means information that is a subset of health information, including demographic information collected from an individual, and
 - (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
 - (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
 - J. “Privacy Standards” means the federal standards for privacy of Individually Identifiable Health Information codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.
 - K. “Protected Health Information” (“PHI”) means Individually Identifiable Health Information that is transmitted by or maintained in Electronic Media, or transmitted or maintained in any other form or medium.
 - L. “Required by Law” means a mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law.
 - M. “Security Incident” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
 - N. “Security Standards” means the federal security standard regulations codified at 45 C.F.R., Parts 160 and 164, Subparts A and C.
 - O. “Unsecured PHI” means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through encryption or destruction.
- 1.2 Capitalized terms used, but not otherwise defined in this Agreement, shall have the meanings ascribed to such terms by the HITECH Act, the Breach Notification Standards, the Privacy Standards or the Security Standards.

ARTICLE II
Permitted Uses

- 2.1 The Business Associate may use PHI received from, or created or received by the Business Associate on behalf of, CHN only in accordance with and for purposes of carrying out its obligations under an Arrangement or as Required by Law.
- 2.2 Except as otherwise provided in or contemplated by an Arrangement or this Agreement, the Business Associate may also:
- A. use PHI received by the Business Associate for the proper management and administration of the Business Associate, or to carry out the legal responsibilities of the Business Associate, provided that such use is permitted by law;
 - B. disclose PHI received by the Business Associate for the proper management and administration of the Business Associate, or to carry out the legal responsibilities of the Business Associate, if (i) the disclosure is Required by Law, or (ii) the disclosure is permitted by law and the Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person agrees to notify the Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached;
 - C. if contemplated by an Arrangement, provide data aggregation services for CHN relating to CHN's health care operations, as such services are defined in 45 C.F.R. § 164.501; and
 - D. if contemplated by an Arrangement, de-identify any and all PHI, provided that the de-identification conforms to the requirements of applicable law as provided for in 45 C.F.R. § 164.514(b) and that the Business Associate maintains such documentation as required by applicable law, as provided for in 45 C.F.R. § 164.514(b).

ARTICLE III
Business Associate Covenants

The Business Associate covenants to:

- 3.1 use and disclose PHI only as necessary to provide services under an Arrangement and only if such use or disclosure, respectively, is in compliance with each applicable requirement of 45 C.F.R. § 164.504(e) and with this Agreement;
- 3.2 not use or further disclose PHI except as permitted or required under an Arrangement, the Privacy Standards and Minnesota law, each as may be amended from time to time;

- 3.3 if the business associate discloses PHI to a business associate that is a subcontractor, it may allow the subcontractor to create, receive, maintain, or transmit PHI on its behalf, provided that the business associate obtains satisfactory assurances that the subcontractor will appropriately safeguard the information. This provision does not constitute CHN's consent for Business Associate to subcontract.
- 3.4 use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for in this Agreement;
- 3.5 mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement;
- 3.6 report to CHN any use or disclosure of the PHI not permitted by an Arrangement or this Agreement of which it becomes aware, with such report to be made in writing immediately upon the Business Associate becoming aware of such use or disclosure;
- 3.7 ensure that any subcontractors or agents to whom it provides PHI received from, or created or received by the Business Associate on behalf of, CHN agree, through a written contract or other written agreement, to the same restrictions and conditions that apply to the Business Associate with respect to the PHI;
- 3.8 make PHI on an individual contained in a Designated Record Set available, in accordance with 45 C.F.R. § 164.524, to CHN and the individual to whom the PHI relates within five (5) days of a request by CHN or the individual for access to the PHI, and if the request for access is from the individual directly, immediately forward such request to CHN, for its records. In addition, if Business Associate uses or maintains an electronic health record ("EHR") as defined in the HITECH Act, in order to comply with Section 13405(e) of the HITECH Act as of its Compliance Date, Business Associate shall provide an electronic copy of an individual's PHI to CHN or the individual, if the individual requests his or her PHI in an electronic format;
- 3.9 within ten (10) days following receipt of a request from CHN for the amendment of an individual's PHI or a record about the individual in a Designated Record Set, the Business Associate shall, as required by 45 C.F.R. § 164.526, incorporate any such amendments in the PHI; provided, however, that CHN has made the determination that the amendment is necessary because the PHI that is the subject of the amendment has been, or foreseeably could be, relied upon by the Business Associate or others to the detriment of the individual who is the subject of the PHI to be amended;
- 3.10 document disclosures of PHI, and within twenty (20) days following notice by CHN to the Business Associate that it has received a request for an accounting of disclosures of PHI regarding an individual, make available to CHN such information in the Business Associate's possession as is required for CHN to make the accounting required by 45 C.F.R. § 164.528, and if the request for an accounting is delivered directly to the Business Associate by an individual, the Business Associate shall, within five (5) days following an individual's request, forward such request to CHN, except when Business Associate is required under federal law and regulations to

- provide an accounting of disclosures made by Business Associate directly to the individual as of the Compliance Date of Section 13405(c) of the HITECH Act;
- 3.11 make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of, CHN available to the Secretary of DHHS for purposes of determining CHN's compliance with the Privacy Standards;
 - 3.12 at termination or expiration of an Arrangement, if feasible, return or destroy all PHI received from, or created or received by the Business Associate on behalf of, CHN which the Business Associate and/or its subcontractors or agents still maintain in any form, and not retain any copies of such information, or if such return or destruction is not feasible, notify CHN of such event in writing, and extend the protections of this Agreement to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible;
 - 3.13 if the parties electronically exchange PHI, Business Associate shall:
 - A. implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic PHI that Business Associate creates, receives, maintains, or transmits on behalf of CHN.
 - B. ensure that any agents or subcontractors to whom Business Associate provides PHI created, received, maintained, or transmitted on behalf of CHN agrees to implement reasonable and appropriate safeguards to protect such PHI;
 - C. report to CHN any Security Incident of which it becomes aware, with such report to be made in writing within five (5) days of the date on which Business Associate becomes aware of the Security Incident; and
 - D. if required by the Security Standards, make its policies and procedures, and documentation required by the Security Standards relating to the security safeguards implemented by Business Associate available to the Secretary of DHHS for purposes of determining CHN's compliance with the Security Standards;
 - 3.14 Comply with the requirements of the Security Standards set forth in 45 C.F.R. § 164.308 (administrative safeguards), 45 C.F.R. § 164.310 (physical safeguards), 45 C.F.R. § 164.312 (technical safeguards) and 45 C.F.R. § 164.316 (security-related policies and procedures and documentation requirements).
 - 3.15 Notwithstanding Section 3.6, notify CHN in writing of any actual or potential Breach of Unsecured PHI and cooperate with CHN, to the extent required by CHN, to provide notice of the Breach under the Breach Notification Standards, in accordance with the following:

- A. Notification that an actual or potential Breach of Unsecured PHI has occurred shall be directed to the CHN Compliance Officer and shall be made within one (1) business day of the day on which the Breach is known to Business Associate;
 - B. As soon as possible, and in any event within no later than fifteen (15) days, Business Associate shall provide to the CHN Compliance Officer written notice with additional detail regarding the actual or potential Breach of Unsecured PHI, which shall include (i) the identification of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed acquired, used or disclosed during the Breach; (ii) a description of what happened; (iii) the date of the Breach; (iv) the date of discovery of the Breach; (v) a description of the types of Unsecured PHI that were involved in the Breach; (vi) a description of what Business Associate is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches; and (vii) any other available information that would be helpful to CHN or that is required for a notification to an individual under 45 C.F.R. § 164.404(c);
 - C. As additional information described in Section 3.15B becomes available to Business Associate at any time after Business Associate has notified CHN of the actual or potential Breach, Business Associate shall immediately notify CHN of such information; and
 - D. If a Law Enforcement Official states to Business Associate that a notification, notice or posting required under the Breach Notification Standards would impede a criminal investigation or cause damage to national security, Business Associate shall comply with the requirements of 45 C.F.R. § 164.412(a) or (b).
- 3.16 Request, use and/or disclose only the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure; provided, that Business Associate shall comply with Section 13405(b) of the HITECH Act as of its Compliance Date;
- 3.17 Not directly or indirectly receive remuneration in exchange for any PHI in compliance with Section 13405(d) of the HITECH Act as of its Compliance Date;
- 3.18 Not make or cause to be made any communication about a product or service that is prohibited by Section 13406 of the HITECH Act as of its Compliance Date; and
- 3.19 Not make or cause to be made any written fundraising communication that is prohibited by Section 13406 of the HITECH Act as of its Compliance Date.

ARTICLE IV
Termination

- 4.1 This Agreement will continue while any Arrangement (or any agreement referenced in Section 5.7) remains in effect with the Business Associate.
- 4.2 Notwithstanding anything to the contrary in this Agreement or an Arrangement, CHN may terminate an Arrangement immediately upon notice to the Business Associate if CHN determines that the Business Associate has violated a material term of this Agreement or otherwise has failed to comply with the Privacy Standards or the Security Standards as they apply to an Arrangement. CHN, in its sole discretion, may, but is not required to, provide the Business Associate with an opportunity to cure the breach within a time acceptable to CHN.
- 4.3 The parties acknowledge that the HIPAA Regulations and the HITECH Act (collectively, the “Standards”) may be modified from time to time. In the event of any such change, both parties agree to promptly enter into good faith negotiations to amend this Agreement, through a written document signed by the parties, to conform to any new or revised legislation, rules and regulations to which the parties are subject. In the event either party does not agree to a reasonable amendment to this Agreement addressing the change in the Standards within thirty (30) days of the change in the Standards, CHN may terminate this Agreement and the Arrangement(s) upon written notice, notwithstanding anything to the contrary in this Agreement or an Arrangement.
- 4.4 Notwithstanding anything to the contrary in this Agreement or an Arrangement, the terms of this Agreement shall survive termination of an Arrangement with respect to the PHI for which return or destruction is not feasible, as provided in Section 3.12 of this Agreement.

ARTICLE V
General

- 5.1 Nothing in this Agreement, including Sections 3.3, 3.7 and 3.13.B, shall permit the Business Associate to assign or subcontract any of its rights or responsibilities under this Agreement or an Arrangement without the prior written consent of CHN.
- 5.2 Nothing in this Agreement shall be construed to create any third party beneficiary rights in any person.
- 5.3 This Agreement may not be modified, nor shall any provision hereof be waived or amended, except by a writing signed by both parties.
- 5.4 CHN is and shall continue to be the owner of all PHI received by the Business Associate from, or created or received by the Business Associate on behalf of, CHN, including any de-identified information received or created by the Business Associate.

- 5.5 Each party agrees to indemnify and hold the other party and the other party's affiliates, and their officers, directors and employees (the "Indemnified Parties") harmless from and against all claims, causes of action, damages, loss, costs and expenses (including fines, penalties and reasonable attorneys' fees) suffered or incurred by any of the Indemnified Parties and arising out of or related to a breach of this Agreement by the indemnifying party, its employees and agents, or its subcontractors, including, but not limited to, costs and expenses incurred by the Indemnified Party in providing notice to individuals of any Breach of Unsecured PHI.
- 5.6 This Agreement is intended to satisfy CHN's obligations under the Standards. If there is a conflict between the terms of this Agreement and any provision of the Standards or if a provision of the Standards that is not included in this Agreement is required to be in this Agreement, such provision shall supersede this Agreement or shall be deemed to be incorporated into this Agreement by reference, and the Business Associate agrees to comply with such provision.
- 5.7 This Agreement applies to each Arrangement and to any agreement, whether oral or written, which is entered into hereafter which renews, extends, replaces or succeeds an Arrangement, and to any other agreement between the parties for which the Standards require such language, unless another agreement meeting the requirements of the Standards is entered into between the parties for such agreement.
- 5.8 To the extent Business Associate performs any activities on behalf of CHN in connection with one or more "Covered Accounts" (as the term is defined in the "Red Flags" Rule at 16 CFR § 681.2(b)(3)) of a Covered Entity, Business Associate shall reasonably cooperate, as requested by CHN, in CHN's investigations under the Red Flags Rule.
- 5.9 To the extent Business Associate is to carry out CHN's obligation(s) under the Privacy Standards, Business Associate must comply with the requirements of the Privacy Standards that apply to CHN in the performance of such obligation.
- 5.10 CHN and Business Associate agree that they are independent contractors and not agents of each other.

**Triple Aim Accountable Care
Organization d/b/a
COMMUNITY HEALTH NETWORK:**

By: _____
Its: _____
Date: _____

By: _____
Its: _____
Date: _____