

HIPAA BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“BAA”) is entered into this ___ day of _____, 202_ (“**Effective Date**”), by and between the **Rochester RHIO** (“RHIO”), located at 200 Canal View Blvd., Ste. 200, Rochester New York 14623 and _____, located at _____ (“Business Associate”), (collectively, the “**Parties**”).

RECITALS

WHEREAS, _____ is a “Business Associate” that is required to comply with the administrative simplification section of the Health Insurance Portability and Accountability Act of 1996 (the “Act”) and its implementing regulations, including the Standards for Privacy of Individually Identifiable Health Information (the “Privacy Rule”) and the Security Standards for the Protection of Electronic PHI (the “Security Rule”), amended by the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) and its implementing regulations, and as they may be further amended from time to time (collectively, “HIPAA”);

WHEREAS, _____ provides professional services for RHIO and such other engagements as shall be entered into between the parties in the future in which RHIO discloses PHI to _____;

WHEREAS, _____, in the course of providing services to RHIO, may have access to certain Protected Health Information (“PHI”) and may be deemed a business associate for certain purposes under HIPAA;

WHEREAS, the Parties contemplate that _____ may obtain PHI, with RHIO’s knowledge and consent, from certain other business associates of RHIO that may possess such PHI; and

WHEREAS, RHIO and _____ are entering into this BAA to set forth _____’s obligations with respect to its handling of the PHI, whether such PHI was obtained from another business associate of _____ or directly from RHIO;

NOW, THEREFORE, for mutual consideration, the sufficiency and delivery of which is acknowledged by the Parties, and upon the premises and covenants set forth herein, the Parties agree as follows:

1. Definitions. Unless otherwise defined herein, capitalized terms used in this BAA shall have the meanings ascribed to them in HIPAA and any other agreement between RHIO and _____, as applicable.

2. Obligations and Activities of Business Associate. To the extent that _____ is provided with or creates any PHI on behalf of RHIO and is acting as a business associate of RHIO, _____ agrees to comply with the provisions of HIPAA applicable to business associates, and in doing so, represents and warrants as follows:

(a) **Use or Disclosure.** _____ agrees to not use or disclose PHI other than as set forth in this BAA, or as required by law.

(b) **Specific Use of Disclosure.** Except as otherwise limited by this BAA, _____ may:

09/30/2020

(i) use or disclose PHI to perform data aggregation to assist RHIO in its operations, as long as such use or disclosure would not violate HIPAA if done by RHIO, or HIPAA permits such use or disclosure by a business associate;

(ii) use or disclose PHI for the proper management and administration of RHIO or to carry out RHIO's legal responsibilities, provided that with respect to disclosure of PHI, such disclosure is required by law, or _____ obtains reasonable assurances from the person to whom the information 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 notifies RHIO of any instances of which it is aware in which the confidentiality of the information has been breached; and

(c) **Minimum Necessary.** _____ agrees to take reasonable efforts to limit requests for, or uses and disclosures of, PHI to the extent practical, a limited data set, otherwise to the minimum necessary to accomplish the intended request, use, or disclosure.

(d) **Safeguards.** _____ shall establish appropriate safeguards, consistent with HIPAA, that are reasonable and necessary to prevent any use or disclosure of PHI not expressly authorized by this BAA.

(i) To the extent that _____ creates, receives, maintains, or transmits Electronic PHI, _____ agrees to establish administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity, as required by the Privacy Rule and Security Rule.

(ii) The safeguards established by _____ shall include securing PHI that it creates, receives, maintains, or transmits on behalf of RHIO, in accordance with the standards set forth in HITECH Act §13402(h) and any guidance issued thereunder.

(iii) _____ agrees to provide RHIO with such written documentation concerning safeguards as RHIO may reasonably request from time to time.

(e) **Agents and Subcontractors.** _____ agrees to obtain written assurances that any agents, including subcontractors, to _____ on behalf of RHIO, agree to the same restrictions and conditions that apply to RHIO with respect to such PHI, including the requirement that it agree to implement reasonable and appropriate safeguards to protect Electronic PHI that is disclosed to it by RHIO.

(f) **Reporting.** Within five (5) business days of discovery by _____, _____ agrees to notify RHIO in writing, of any use or disclosure of or Security Incident involving PHI, including any Breach of Unsecured PHI, not provided for by this BAA, of which Business Associate may become aware.

(i) In the notice provided to RHIO by _____ regarding unauthorized uses and/or disclosures of PHI, _____ shall describe the remedial or proposed mitigation efforts required under Section 2(g) of this BAA.

(ii) Specifically with respect to reporting a Breach of Unsecured PHI, _____ agrees to include the identity of the individual(s) whose Unsecured PHI was Breached in the written notice provided to RHIO, and any additional information required by HIPAA.

(ii) _____ agrees to cooperate with RHIO upon report of any such Breach so that RHIO may provide the individual(s) affected by such Breach with proper notice as required by HIPAA.

(g) **Mitigation.** _____ agrees to mitigate, to the extent practicable, any harmful effect that is known to _____ resulting from a use or disclosure of PHI by _____ in violation of the requirements of this BAA.

(h) **Audits and Inspections.** _____ agrees to make its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI available to the Secretary, in a time and manner mutually agreed to by the Parties or designated by the Secretary, for purposes of the Secretary determining the Business Associates' compliance with HIPAA.

(i) **Accounting.** _____ agrees to document and report to RHIO, within fourteen (14) days, _____'s disclosures of PHI so RHIO can comply with its accounting of disclosure obligations in accordance with 45 C.F.R. §164.528 and any subsequent regulations issued thereunder.

(j) **Designated Record Set.** While the Parties do not intend for _____ to maintain any PHI in a designated record set, to the extent that _____ does maintain any PHI in a designated record set, _____ agrees to make available to RHIO, such PHI within fourteen (14) days:

(i) for RHIO to comply with its access obligations in accordance with 45 C.F.R. §164.524, the 21st Century Cures Act and any subsequent regulations issued thereunder; and

(ii) for amendment upon RHIO's request and incorporate any amendments to PHI as may be required for RHIO to comply with its amendment obligations in accordance with 45 C.F.R. §164.526 and any subsequent guidance.

3. Obligations of Rochester RHIO.

(a) RHIO agrees to notify _____ of any limitation(s) in RHIO's Notice of Privacy Practices in accordance with 45 C.F.R. §164.520, to the extent that such limitation may affect _____'s use or disclosure of PHI.

(b) RHIO agrees to notify _____ of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect _____'s use or disclosure of PHI.

(c) RHIO agrees to notify _____ of any restriction to the use or disclosure of PHI that RHIO has agreed to in accordance with 45 C.F.R. §164.522, to the extent that such restriction may affect _____'s use or disclosure of PHI.

(d) RHIO agrees to allow use, disclosure, and requests of PHI under this BAA to a limited data set or, if needed by _____, to the Minimum Necessary PHI to accomplish the intended purpose of such use, disclosure, or request, however, in compliance with the 21st Century Cures Act, will not interfere with, cause unnecessary delay or unreasonably restrict or prohibit access to PHI.

4. Term and Termination.

(a) **Term.** This BAA shall become effective upon the Effective Date and, unless otherwise terminated as provided herein, shall have a term that shall run concurrently with that of the last expiration date.

(b) **Termination Upon Breach.**

(i) Without limiting the termination rights of the Parties, upon either Party's knowledge of a material breach by the other Party to this BAA, the breaching Party shall notify the non-breaching Party of such breach and the breaching party shall have fourteen (14) days from the date of notification to the non-breaching party to cure such breach. In the event that such breach is not cured, or cure is infeasible, the non-breaching party shall have the right to immediately terminate this BAA.

(c) **Termination by Either Party.** Either Party may terminate this BAA upon provision of thirty (30) days' prior written notice.

(d) **Effect of Termination.**

(i) To the extent feasible, upon termination of this BAA, _____ agrees, and shall cause any subcontractors or agents to return or destroy and retain no copies of any PHI received from, or created or received by _____ on behalf of RHIO. _____ agrees to complete such return or destruction as promptly as possible and verify in writing within thirty (30) days of the termination of this BAA to RHIO that such return or destruction has been completed.

(ii) If not feasible, _____ agrees to provide RHIO notification of the conditions that make return or destruction of PHI not feasible. Upon notice to RHIO that return or destruction of PHI is not feasible, _____ agrees to extend the protections of this BAA to such PHI for as long as _____ maintains such PHI.

5. Miscellaneous.

(a) **Regulatory References.** A reference in this BAA to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.

(b) **Amendment.** The Parties acknowledge that the provisions of this BAA are designed to comply with HIPAA and agree to take such action as is necessary to amend this BAA from time to time as is necessary for RHIO to comply with the requirements of HIPAA. Regardless of the execution of a formal amendment of this BAA, the BAA shall be deemed amended to permit RHIO and _____ to comply with HIPAA.

(c) **Method of Providing Notice.** Any notice required to be given pursuant to the terms and provisions of this BAA shall be in writing and may be either personally delivered or sent by registered or certified mail in the United States Postal Service, Return Receipt Requested, postage prepaid, addressed to each Party at the addresses listed in the BAA. Any such notice shall be deemed to have been given if mailed as provided herein, as of the date mailed.

(d) **Parties Bound.** This BAA shall inure to the benefit of and be binding upon the Parties hereto and their respective legal representatives, successors, and assigns. _____ may not assign or subcontract the rights or obligations under this BAA without the express written consent of RHIO. RHIO may assign its rights and obligations under this BAA to any successor or affiliated entity.

(e) **No Waiver.** No provision of this BAA or any breach thereof shall be deemed waived unless such waiver is in writing and signed by the Party claimed to have waived such provision or breach. No waiver of a breach shall constitute a waiver of or excuse any different or subsequent breach.

(f) **Complete Agreement.** This BAA constitutes the complete agreement between the Parties and supersedes all prior representations or agreements, whether oral or written, with respect to such matters. No oral modification or waiver of any of the provisions of this BAA shall be binding on either party. No obligation on either party to enter into any transaction is to be implied from the execution or delivery of this BAA.

(g) **Interpretation.** Any ambiguity in this BAA shall be resolved to permit the parties to comply with HIPAA and any subsequent guidance.

(h) **No Third Party Rights.** The terms of this BAA are not intended nor should they be construed to grant any rights, remedies, obligations, or liabilities whatsoever to parties other than RHIO and _____ and their respective successors or assigns.

(i) **Applicable Law.** This BAA shall be governed under the laws of the State of New York, without regard to choice of law principles.

(j) **Judicial and Administrative Proceedings.** In the event that _____ receives a subpoena, court or administrative order, or other discovery request or mandate for release of PHI, _____ agrees to collaborate with RHIO_ with respect to _____'s response to such request. _____ shall notify RHIO within seven (7) days of receipt of such request or mandate.

(k) **Transmitting Electronic PHI.** Electronic PHI transmitted or otherwise transferred from between RHIO and _____ must be encrypted by a process that renders the Electronic PHI unusable, unreadable, or indecipherable to

unauthorized individuals within the meaning of HITECH Act § 13402 and any implementing guidance including, but not limited to, 45 C.F.R. § 164.402.

6. IN WITNESS WHEREOF, the Parties hereto have executed this BAA to be effective on the date set forth above.

By: _____
Name: _____
Title: _____
Address: _____

Date: _____

Rochester RHIO
By: _____
Name: _____
Title: _____
Address: 200 Canal View Blvd., Ste. 200
Rochester, New York 14623
Date: _____