

## BUSINESS ASSOCIATE AGREEMENT

**THIS AGREEMENT** is made effective as of the \_\_\_\_ day of \_\_\_\_\_ 202\_\_ by and between **ROCHESTER RHIO**, (the "Business Associate"), located at 200 Canal View Blvd., Ste. 200, Rochester, New York 14623 and \_\_\_\_\_, (the "Subcontracted Business Associate"), located at \_\_\_\_\_, collectively, the "**Parties**".

**WHEREAS**, the Business Associate has entered into an agreement with \_\_\_\_\_, a Covered Entity under which the Business Associate provides services to \_\_\_\_\_ and, in the course of providing those services, the Business Associate may or will have access to certain confidential protected health information in the course of providing services to \_\_\_\_\_ concerning the individuals to whom \_\_\_\_\_ provides care (each referred to as an "Individual"), and such information includes information created or received by \_\_\_\_\_, or created, maintained, transmitted or received by the Business Associate, or created, maintained, transmitted or received by Subcontracted Business Associate, (the "PHI"), and includes electronic protected health information ("E PHI"); and

**WHEREAS**, as a result of their Access to and Use and Disclosure of PHI and E PHI, the Business Associate and Subcontracted Business Associate acknowledge that they are obligated to comply with the applicable provisions of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations including, but not limited to, the Security Standards for the Protection of Electronic Protected Health Information (the "Security Rules") and the Privacy of Individually Identifiable Health Information standards (the "Privacy Rules") (collectively the "HIPAA Requirements"); and

**WHEREAS**, the parties are obligated under the HIPAA Requirements to enter into a written agreement under which Subcontracted Business Associate will agree to appropriately protect and safeguard PHI and E PHI; and

**WHEREAS**, Subcontracted Business Associate and the Business Associate have entered into an agreement (the "Contract"), under which Subcontracted Business Associate provides services to the Business Associate and, in the course of providing those services, Subcontracted Business Associate may or will have access to PHI and E PHI; and

**WHEREAS**, the Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009 includes new standards and has new implementing regulations which provide that certain provisions of the HIPAA Requirements are directly applicable to business associates and that any existing business associate agreements must be updated to address these new standards (collectively referred to as the "HITECH Act"); and

**WHEREAS**, the HIPAA Requirements and the new provisions of the HITECH Act shall collectively be known in this Agreement as the "HIPAA Rules";

**NOW, THEREFORE**, the parties agree as follows:

1. **Definitions**

[Type here]

(a) Covered Entity. “Covered Entity” shall have the same meaning as the term “covered entity” is defined in the HIPAA Rules, 45 CFR 160.103.

(b) Business Associate. “Business Associate” shall have the same meaning as the term “business associate” is defined in the HIPAA Rules, 45 CFR 160.103.

(c) Subcontracted Business Associate. “Subcontracted Business Associate” shall have the same meaning as the term “business associate” is defined in the HIPAA Rules, 45 CFR 160.103.

(d) The following capitalized terms and/or their derivatives used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Disclosure, Electronic Protected Health Information/EPHI, Health Care Operations, Individual, Limited Data Set, Minimum Necessary, Notice of Privacy Practices, Protected Health Information/PHI, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

## 2. Use and Disclosure of PHI and EPHI

(a) Subcontracted Business Associate will hold and keep PHI and EPHI strictly confidential and Use and/or Disclose PHI and EPHI only as required or permitted under the terms of the Contract, this Agreement, and the HIPAA Rules. The HIPAA Rules address the Use and/or Disclosure of PHI and EPHI by the Business Associate, and also apply to Subcontracted Business Associate and Subcontracted Business Associate’s Subcontractors that create, receive, transmit or maintain PHI and/or EPHI in order to perform a function, activity or service delegated by Subcontracted Business Associate. Any Use and/or Disclosure must be associated with the treatment of the Individual to whom the PHI and EPHI relates, payment for the treatment of that Individual, or the Business Associate’s general Health Care Operations.

(b) Subcontracted Business Associate may also Use and/or Disclose the PHI and EPHI for the proper management and administration of Subcontracted Business Associate, or to carry out the legal responsibilities of Subcontracted Business Associate. However, such Use and/or Disclosure must be either Required By Law or, prior to making Use of the PHI and EPHI or Disclosing the PHI and EPHI, Subcontracted Business Associate must obtain reasonable assurances from the person/entity to whom the PHI and EPHI will be Disclosed that the PHI and EPHI: (i) will be held confidentially and Used or further Disclosed only as Required By Law or for the purpose for which it was Disclosed; and (ii) the person to whom it is Disclosed agrees to notify Subcontracted Business Associate of any instance of which it is aware in which the confidentiality of the PHI and EPHI has been Breached.

(c) Subcontracted Business Associate may also Use the PHI and EPHI to provide Data Aggregation services to the Business Associate. Data Aggregation means, with respect to PHI and EPHI, the combining of the PHI and EPHI by Subcontracted Business Associate with Protected Health Information received by Subcontracted Business Associate in its capacity as a business associate of another health care provider to permit data analysis that relates to the Health Care Operations of the Business Associate and the other health care provider.

(d) Subcontracted Business Associate shall not Use or further Disclose the PHI and electronic PHI other than as permitted or required by this Agreement. Data shall only be used for purposes of Treatment, Payment or Operations for the mutual customers of the Parties, pursuant to 45 CFR 164.506. Any other usage of the data constitutes Secondary Use of the data. Subcontracted Business Associate shall not engage in Secondary Use of the PHI or electronic PHI unless previously authorized by Rochester RHIO, in writing.

### 3. **Business Associate's Obligations**

(a) Business Associate shall notify Subcontracted Business Associate of any limitation(s) in the Notice of Privacy Practices of Business Associate, to the extent that such limitation may affect Subcontracted Business Associate's Use or Disclosure of PHI and EPHI.

(b) Business Associate shall notify Subcontracted Business Associate of any changes in, or revocation of, the permission by an Individual to Use or Disclose their PHI and/or EPHI, to the extent that such changes may affect Subcontracted Business Associate's Use or Disclosure of PHI and EPHI.

(c) Business Associate shall notify Subcontracted Business Associate of any restriction on the Use or Disclosure of PHI and EPHI that Business Associate has agreed to or is required to abide by, to the extent that such restriction may affect Subcontracted Business Associate's Use or Disclosure of PHI and EPHI. However, Business Associate and Subcontracted Business Associate must comply with the provisions set forth in the 21<sup>st</sup> Century Cures Act, including, but not limited to the provisions prohibiting Information Blocking.

### 4. **Safeguards/Requirements**

(a) Subcontracted Business Associate will use appropriate safeguards to prevent any Use or Disclosure of the PHI and EPHI that is not permitted under the terms of this Agreement. Specifically, Subcontracted Business Associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI and EPHI that it creates, receives, maintains or transmits on behalf of the Business Associate.

(b) Subcontracted Business Associate will ensure that any of its agents, including a Subcontractor, to whom Subcontracted Business Associate discloses PHI and EPHI, will enter into a Subcontracted Business Associate Agreement with Subcontracted Business Associate and agree to the same restrictions and conditions that apply to Subcontracted Business Associate under the terms of this Agreement, and will agree to implement reasonable and appropriate safeguards as required by the HIPAA Rules to protect the PHI and EPHI.

(c) Subcontracted Business Associate may Use and Disclose PHI and/or EPHI that Subcontracted Business Associate obtains, maintains, transmits or creates only if such Use or Disclosure is in compliance with each applicable requirement of the HIPAA Rules relating to business associate agreements. The additional requirements of the

HITECH Act that relate to privacy and that are made applicable to Business Associate shall also be applicable to Subcontracted Business Associate. Subcontracted Business Associate shall comply with these privacy requirements which shall be incorporated into this Agreement. Business Associate and Subcontracted Business Associate may not enter into any agreement that violates the terms of the 21<sup>st</sup> Century Cures Act, including the provision prohibiting Information Blocking.

(d) Under the HIPAA Rules the requirements pertaining to “administrative safeguards,” “physical safeguards,” “technical safeguards,” and “policies and procedures and documentation requirements” of the Security Rules apply to Subcontracted Business Associate in the same manner that such sections apply to Business Associate, and the additional requirements of the HITECH Act that relate to security and that are made applicable to Business Associate shall also be applicable to Subcontracted Business Associate. Subcontracted Business Associate shall comply with these security requirements which shall be incorporated into this Agreement.

(e) Unless Business Associate agrees, in writing, that this HITECH Act requirement is not feasible with respect to particular PHI or EPHI, Subcontracted Business Associate shall secure all PHI and EPHI by utilizing a technology standard or methodology that renders PHI and EPHI unusable, unreadable, or indecipherable to unauthorized individuals and is consistent with guidance, as further amended in the future, issued by the Secretary of the Department of Health and Human Services (the “Secretary”) specifying the technologies and methodologies that render PHI and EPHI unusable, unreadable, or indecipherable to unauthorized individuals.

(f) Except as otherwise allowed in this Agreement and the HIPAA Rules, Subcontracted Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI or EPHI of an Individual unless the Individual has provided a valid, HIPAA-compliant authorization, including a specification of whether the PHI or EPHI can be further exchanged for remuneration by the receiving party.

(g) Except as otherwise provided in the HIPAA Rules, Subcontracted Business Associate shall not directly or indirectly receive payment in exchange for making certain communications to Individuals about a product or service that encourages the recipient to purchase or use the product or service.

(h) Subcontracted Business Associate will report to Business Associate's Privacy and/or Security Official, within five (5) business days, any Use or Disclosure of PHI and EPHI not provided for by this Agreement. Subcontracted Business Associate shall conduct and document a risk assessment, in accordance with the HIPAA Rules, of such unauthorized Use or Disclosure and provide Business Associate with a copy of such risk assessment upon Business Associate's request. In the event Subcontracted Business Associate concludes the unauthorized Use or Disclosure constitutes a Breach of Unsecured PHI, Subcontracted Business Associate shall provide to Business Associate the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Subcontracted Business Associate to have been, Accessed, Used, acquired, or Disclosed during such Breach, as well as such other information required by the HIPAA Rules. A Breach shall be treated as discovered by Subcontracted Business Associate as of the first day on which such Breach is known to such Subcontracted Business Associate

(including any person, other than the individual committing the Breach, that is an employee, officer, or other agent of Subcontracted Business Associate) or should reasonably have been known to Subcontracted Business Associate to have occurred.

(i) Business Associate, in its sole and absolute discretion, may elect to delegate to Subcontracted Business Associate the requirement under the HIPAA Rules to notify affected Individuals of a Breach of Unsecured Protected Health Information if such Breach results from, or is related to, an act or omission of Subcontracted Business Associate or the agents or representatives of Subcontracted Business Associate. If Business Associate elects to make such a delegation, Subcontracted Business Associate shall perform such notifications and undertake all related remediation activities that are reasonably required (i) at Subcontracted Business Associate's sole cost and expense, and (ii) in compliance with all applicable requirements, including the HIPAA Rules. Subcontracted Business Associate shall also provide Business Associate with the opportunity, in advance, to review and approve of the form and content of any such Breach notification that Subcontracted Business Associate provides to Individuals.

(j) Subcontracted Business Associate will respond to a request for, changes in, or a revocation of, permission by an Individual to restrict Subcontracted Business Associate's Use or Disclosure of PHI or EPHI, in a timely manner in accordance with the HIPAA Rules, and to make changes to Subcontracted Business Associate's procedures to the extent that such request, if approved, may affect Subcontracted Business Associate's Use or Disclosure of PHI or EPHI. Subcontracted Business Associate will monitor compliance with these requests for restrictions in accordance with the HIPAA Rules. Business Associate and Subcontracted Business Associate shall comply with all requirements set forth in the 21<sup>st</sup> Century Cures Act, including the prohibition against Information Blocking.

(k) Subcontracted Business Associate will Use, Disclose, or request PHI or EPHI, only if it limits such PHI or EPHI, to the extent practicable, to a Limited Data Set, or, if needed by the entity, to the Minimum Necessary to accomplish the intended purposes of such Use, Disclosure, or request. In the case of the Disclosure of PHI or EPHI, Subcontracted Business Associate, in conjunction with the Business Associate, shall determine what constitutes the Minimum Necessary to accomplish the intended purposes of such Disclosure. Business Associate and Subcontracted Business Associate shall comply with all requirements set forth in the 21<sup>st</sup> Century Cures Act, including the prohibition against Information Blocking.

(l) Subcontracted Business Associate recognizes the civil and criminal penalties for a violation of the HIPAA Rules, shall apply to Subcontracted Business Associate with respect to such violation in the same manner as such penalties apply to the Business Associate.

(m) Subcontracted Business Associate will comply with any periodic audit request initiated by the Secretary to ensure that Subcontracted Business Associate is complying with the HIPAA Rules.

(n) Subcontracted Business Associate will not acquire any title or rights to the PHI or EPHI, including any de-identified information, as a result of this Agreement.

(o) Subcontracted Business Associate will immediately report to the Business Associate any Use or Disclosure of the PHI and EPHI that is not permitted under the terms of this Agreement, provided that Subcontracted Business Associate becomes aware of such improper Use or Disclosure. Subcontracted Business Associate will also immediately report to the Business Associate any Security Incident of which it becomes aware.

5. **Access to Information**

(a) Subcontracted Business Associate will make its internal books and records relating to the Use and Disclosure of PHI and EPHI available to the Business Associate and to the Secretary, for the purpose of the Secretary determining whether the Business Associate has complied with the HIPAA Rules, at the request of the Business Associate and at a time and in a manner designated by the Business Associate.

(b) Subcontracted Business Associate will provide access to PHI and EPHI in its possession to the Business Associate or, as directed by the Business Associate, to an Individual, in order to meet the Business Associate's obligations to provide access to the PHI and EPHI to the Individual. Access will be provided at the request of the Business Associate and at a time and in a manner designated by the Business Associate, in compliance with the 21<sup>st</sup> Century Cures Act.

(c) Subcontracted Business Associate will provide access to PHI and EPHI in its possession to the Business Associate, or as directed by the Business Associate, so that the Business Associate can amend the PHI and EPHI as required under the HIPAA Rules. Access will be provided at the request of the Business Associate and at a time and in a manner designated by the Business Associate. Subcontracted Business Associate will also make any amendment to the PHI and EPHI that is requested by the Business Associate as a result of the Individual having requested such an amendment.

(d) Subcontracted Business Associate will provide access to PHI and EPHI in its possession to the Business Associate or, as directed by the Business Associate, in order for the Business Associate to provide an Accounting of Disclosures which it is required to do under the HIPAA Rules. Access will be provided at the request of the Business Associate and at a time and manner designated by the Business Associate.

6. **Mitigation**

Subcontracted Business Associate will mitigate, to the extent practicable, any harmful effect that is known to Subcontracted Business Associate of a Use or Disclosure of PHI or EPHI by Subcontracted Business Associate in violation of the terms of this Agreement.

7. **Indemnification**

Subcontracted Business Associate will indemnify, defend, and hold harmless Business Associate and Business Associate's employees, directors, officers, Subcontractors, agents, or members of its workforce (each of the foregoing referred to as an "Indemnified Party") during the term of this Agreement and subsequent to its termination, from and against all claims,

damage, losses, liabilities, fines, penalties, costs or expenses including, but not limited to, expenses associated with State and/or Federal Breach notification requirements and reasonable attorneys' fees (collectively, "Losses") suffered by an Indemnified Party that arises from, or is connected with, any act or omission by Subcontracted Business Associate or Subcontracted Business Associate's employees, agents, Subcontractors or representatives that constitutes or that is otherwise asserted by any regulatory agency or third party to be (i) a breach of any term or condition of this Agreement, (ii) negligence or misconduct, and/or (iii) a violation of the HIPAA Rules. The provisions of this paragraph shall survive the expiration or termination of this Agreement for any reason.

8. **Termination**

(a) The Contract may be terminated by the Business Associate if the Business Associate determines that Subcontracted Business Associate has materially breached its obligation(s) under this Agreement. If termination is not a feasible remedy for the Business Associate, the Business Associate may report the breach by Subcontracted Business Associate to the Secretary.

(b) Upon termination or expiration of this Agreement for any reason, Subcontracted Business Associate, with respect to PHI and EPHI received from Business Associate, or created, maintained, or received by Subcontracted Business Associate on behalf of Business Associate, shall:

1) Retain only that PHI and EPHI which is necessary for Subcontracted Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

2) Return to Business Associate or, if agreed to by Business Associate, destroy the remaining PHI and EPHI that Subcontracted Business Associate still maintains in any form;

3) Continue to use appropriate safeguards and comply with the HIPAA Rules with respect to PHI and EPHI to prevent Use or Disclosure of PHI and EPHI, other than as provided for in this Section, for as long as Subcontracted Business Associate retains the PHI;

4) Not Use or Disclose the PHI or EPHI retained by Subcontracted Business Associate other than for the purposes for which such PHI and EPHI was retained and subject to the same conditions set forth in this Agreement which applied prior to expiration or termination; and

5) Return to Business Associate or, if agreed to by Business Associate, destroy the PHI and EPHI retained by Subcontracted Business Associate when it is no longer needed by Subcontracted Business Associate for its proper management and administration or to carry out its legal responsibilities or, if such return or destruction is not feasible, extend the protections of this Agreement to the PHI and EPHI and limit further Uses and Disclosures to those purposes that make the return or the destruction of the PHI and EPHI not feasible.

(c) Survival. The obligations of Subcontracted Business Associate under this Section shall survive the expiration or termination of this Agreement.

9. **Miscellaneous**

The following provisions shall apply to this Agreement:

(a) All capitalized and other terms used but not otherwise defined in this Agreement shall have the same meaning as those terms contained in the HIPAA Rules.

(b) The paragraph headings contained in this Agreement have been prepared for convenience of reference only and shall not control, affect the meaning, or be taken as an interpretation of any provision of this Agreement.

(c) Several copies of this Agreement may be executed by the parties, each of which shall be deemed an original for all purposes, and all of which together shall constitute but one and the same instrument.

(d) The parties will take such action as is necessary to amend or further amend, as the case may be, this Agreement from time to time as is necessary for Business Associate and Subcontracted Business Associate to comply with the HIPAA Rules, as further amended in the future. Any ambiguity or inconsistency in this Agreement shall be resolved to permit Business Associate to comply with the requirements of the HIPAA Rules.

(e) In the event any term or condition of this Agreement should be breached by either party and thereafter waived by the other party, then such waiver shall be limited to the particular breach so waived and shall not be deemed to waive any other breach either prior or subsequent to the breach so waived.

10. **Failure of Performance**

If either party to this Agreement fails in the due performance of any of its obligations under the terms of this Agreement, the other party will have the right, at its election, to sue for damages for such breach and to seek such legal and equitable remedies as may be available to it, including the right to recover all reasonable expenses, which shall include reasonable attorneys' fees, legal expenses and court costs, incurred: (a) to sue for damages; (b) to seek such other legal and equitable remedies; and (c) to collect any damages and enforce any court order or settlement agreement including, but not limited to, additional application to the court for an order of contempt. Nothing contained herein shall be construed to restrict or impair the rights of either party to exercise this election. All rights and remedies herein provided or existing at law or in equity shall be cumulative of each other and may be enforceable concurrently therewith or from time to time.



11. **Notices**

Any notice or other communication which is required to be given under the terms of this Agreement shall be in writing and shall be delivered personally, or sent by registered mail, or by certified mail return receipt requested to the addresses of each party set forth in the beginning of this Agreement. Any notice which is mailed shall be deemed to have been given on the second business day after the day of mailing (not counting the day mailed), irrespective of the date of receipt. Notices may be signed and given by the attorney for the party sending the notice. A new address may be designated by notice.

12. **Construction**

(a) All understandings and agreements previously made by and between the parties are merged in this Agreement, which alone fully and completely expresses their agreement. This Agreement supersedes and replaces any such previously executed Pre-Existing Subcontracted Business Associate Agreement. This Agreement shall not change or modify any rights or obligations of Business Associate or Subcontracted Business Associate that may have accrued under a Pre-Existing Subcontracted Business Associate Agreement while such agreement was in effect.

(b) This Agreement may not be changed, terminated, nor any of its provisions modified or waived, except in writing signed by all of the parties to this Agreement. Any provisions of this Agreement which by their terms are intended to survive the termination or expiration of this Agreement shall so survive.

13. **Applicable Law; Jurisdiction; Venue**

This Agreement will be governed by and construed in accordance with the laws of the State of New York without regard to its principles of conflicts of law or without regard to any custom or rule of law requiring construction against the drafter. The County of residence of the Business Associate in the State of New York is hereby designated as the exclusive forum for any action or proceeding arising from or in any way connected to this Agreement, and the parties hereby expressly consent to the personal jurisdiction of the state or federal courts in this forum.

**15. Binding Effect**

This Agreement shall be binding upon and will inure to the benefit of the parties, their officers, directors, successors and assigns.

**IN WITNESS WHEREOF**, we have signed this Business Associate Agreement.

\_\_\_\_\_

**ROCHESTER RHIO**

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Signature: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_