

PatientStudio Business Associate Agreement

This Business Associate Agreement (hereinafter referred to as "BAA") is entered into between Member ("Covered Entity") and Bartley & Sanborn, DBA PatientStudio, a Virginia Limited Liability corporation ("Business Associate").

Whereas Business Associate performs functions, activities, or services for or on behalf of Covered Entity, and Business Associate creates, receives, maintains, or transmits Protected Health Information ("PHI"), including Electronic Protected Health Information ("EPHI"), in order to perform such functions, activities, or services (referred to collectively as the "Services");

Whereas the purpose of this BAA is to set forth the terms and conditions of PHI disclosure by Covered Entity to Business Associate, to set forth the terms and conditions of Business Associate's use and disclosure of PHI, and to ensure the confidentiality, integrity, and availability of EPHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity;

Whereas it is the intent of Covered Entity and Business Associate that this BAA will meet the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the American Recovery and Reinvestment Act of 2009, Public Law 111-5 ("ARRA"), the Privacy Rule, the Security Rule, 45 C.F.R. Parts 160 and 164, and the Final HIPAA Omnibus Rule.

Now, therefore, in consideration of the mutual promises set forth in this BAA and other good and valuable consideration (the sufficiency and receipt of which are hereby severally acknowledged), the parties agree as follows:

1. Definitions. Unless otherwise specified in this BAA, all capitalized terms not otherwise defined shall have the meanings established in Title 45, Parts 160 and 164, of the United States Code of Federal Regulations, as amended from time to time, and/or in the American Recovery and Reinvestment Act of 2009 ("ARRA"). For purposes of clarification, the following terms shall have the definitions set forth below:
 - a. "Privacy Standards" shall mean the Standards for Privacy of Individually Identifiable Health Information as set forth in 45 C.F.R. Parts 160 and 164.
 - b. "Security Standards" shall mean the Security Standards for the Protection of Electronic Protected Health Information as set forth in 45 C.F.R. Parts 160 and 164.
 - c. "Subcontractor" shall mean a person or entity to whom Business Associate delegates a function, activity, or service involving the creation, receipt, maintenance, or transmission of PHI on behalf of Business Associate, other than as a member of Business Associate's workforce.
2. Business Associate Obligations. Business Associate may create, receive, maintain, or transmit from or on behalf of Covered Entity health information that is protected under applicable state and/or federal law, including, without limitation, PHI. Business Associate shall not Use or Disclose the PHI other than as permitted or required by this BAA or as Required by Law. Business Associate agrees not

to Use or Disclose (or permit the Use or Disclosure of) PHI in a manner that would violate the requirements of the Privacy Standards or the Security Standards if the PHI were Used or Disclosed by Covered Entity in the same manner, except as provided in Sections 3 and 4 of this BAA.

3. Use of PHI.

a. Administrative and Other Duties. Business Associate may Use PHI as necessary (i) for performing Services on behalf of Covered Entity, (ii) for the proper management and administration of the Business Associate, and (iii) for carrying out Business Associate's legal responsibilities, provided in each case that such Uses are permitted under federal and state law.

b. Data Aggregation. Business Associate may provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B) and to Use, Disclose, and combine PHI created or received on behalf of Covered Entity by Business Associate pursuant to this BAA with PHI received by Business Associate in its capacity as a business associate of other covered entities, to permit data analyses that relate to the Health Care Operations of the respective covered entities and/or Covered Entity.

c. De-Identified PHI. Business Associate may de-identify any and all PHI created or received by Business Associate under this BAA. PHI that has been de-identified within the meaning of 45 CFR § 164.514(b) is no longer PHI and may be used or disclosed by Business Associate for any lawful purpose.

4. Disclosure of PHI. Business Associate may Disclose PHI as necessary to perform Services on behalf of Covered Entity. Additionally, Business Associate may Disclose PHI (i) for the proper management and administration of the Business Associate and (ii) to carry out Business Associate's legal responsibilities, provided that either (a) the Disclosure is Required by Law or (b) the Business Associate obtains reasonable assurances from the person to whom the information is Disclosed that the information 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 and such person agrees to immediately notify the Business Associate of any instances of which he or she is aware that the confidentiality of the information has been breached. Business Associate will determine the amount of PHI necessary to accomplish the intended purpose of disclosure and will make reasonable efforts to limit the receipt, use, and disclosure of PHI to the minimum necessary as required by the Privacy Laws.

5. Reports. Business Associate agrees to report to Covered Entity:

a. Breaches of Unsecured PHI. Any Breach of Unsecured PHI. Each report of a Breach of Unsecured PHI Discovered by Business Associate, unless delayed for law enforcement purposes, shall be made without delay and in no case later than thirty (30) calendar days after Discovery of the Breach. Such report shall include 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 such Breach and any other available

information Covered Entity is required to include in notification to the affected Individual(s) under 45 C.F.R. § 164.404(c);

b. Unauthorized Uses and Disclosures. Any Use or Disclosure of PHI not provided for by this BAA of which Business Associate becomes aware, without unreasonable delay and in no case later than ten (10) business days after Business Associate becomes aware of it; and

c. Security Incidents. Any successful Security Incident of which Business Associate becomes aware, without unreasonable delay. The parties acknowledge and agree that this Section 5(c) constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents, for which no additional notice shall be required. "Unsuccessful Security Incidents" means, without limitation, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, so long as no such incident results in unauthorized access, acquisition, Use, or Disclosure of PHI.

6. Safeguards. Business Associate will use appropriate safeguards and comply, where applicable, with 45 C.F.R. 164 Subpart C with respect to EPHI to prevent Use or Disclosure of the information other than as provided for by this BAA.

7. Individual Rights to Access and Amend.

a. Access. If Business Associate maintains a Designated Record Set on behalf of Covered Entity, Business Associate shall permit an Individual to inspect or copy PHI contained in that Designated Record Set about the Individual in accordance with the Privacy Standards set forth in 45 C.F.R. § 164.524, as it may be amended from time to time unless excepted or a basis for denial exists under 45 C.F.R. § 164.524, as determined by the Covered Entity. In the event that a Business Associate uses or maintains an Electronic Health Record on behalf of Covered Entity, then an Individual's right of access under 45 C.F.R. § 164.524 shall include the right to obtain a copy of the PHI in an electronic format—if the Individual chooses in a clear, conspicuous, and specific manner to direct the Business Associate to transmit such copy to any person designated by the Individual. Business Associate shall respond to any request from Covered Entity for access by an Individual within five (5) days of such request unless otherwise agreed to by Covered Entity. The information shall be provided in the form or format requested (if it is readily producible in such form or format) or in summary if the Individual has agreed in advance to accept the information in summary form. A reasonable, cost-based fee may be charged for copying PHI or providing a summary of PHI in accordance with 45 C.F.R. § 164.524(c)(4), provided that any such fee relating to a copy or summary of PHI is not greater than the labor, supplies, and postage costs incurred in response to the request for the copy or summary.

b. Amendment. Business Associate shall accommodate an Individual's right to amend PHI about the Individual in a Designated Record Set in accordance with the Privacy Standards set forth at 45 C.F.R. § 164.526, as it may be amended from time to time unless excepted or a basis

for denial exists under 45 C.F.R. § 164.526, as determined by the Covered Entity. Covered Entity shall determine whether a denial of an amendment request is appropriate or an exception applies. Business Associate shall notify Covered Entity within five (5) days of receipt of any request for amendment by an Individual and shall make any amendment requested by Covered Entity within ten (10) days of such request. Business Associate shall have a process in place for handling requests for amendments and for appending such requests to the Designated Record Set when required by 45 C.F.R. § 164.526.

8. Accounting of Disclosures. Business Associate shall document Disclosures of PHI, and information related to such Disclosures, as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. Business Associate shall provide such documentation to Covered Entity within ten (10) business days of Covered Entity's written request, to enable Covered Entity to respond to such a request for an accounting. If an Individual submits a request for an accounting directly to Business Associate, Business Associate shall forward the request to Covered Entity within five (5) business days.
9. Compliance with Law. To the extent Business Associate is to carry out Covered Entity's obligation under the Privacy Standards, Business Associate shall comply with the requirements of the Privacy Standards that apply to Covered Entity in the performance of such obligation.
10. Prohibition of Sale of PHI and use of PHI for Marketing. Business Associate will not directly or indirectly receive remuneration in exchange for any PHI, nor will it Use or Disclose PHI for fundraising and/or marketing purposes, except with the Covered Entity's prior written consent and in accordance with applicable Privacy Laws.
11. Subcontractors. In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), Business Associate shall ensure that any Subcontractor that creates, receives, maintains, or transmits PHI on behalf of Business Associate agrees in writing to restrictions and conditions substantially similar to those that apply to Business Associate under this BAA with respect to such PHI, including the implementation of reasonable and appropriate safeguards to protect EPHI.
12. Access to Books and Records. Business Associate shall make its internal practices, books, and records relating to the Use and Disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance with the Privacy Standards and this BAA.
13. Term and Termination.
 - a. PHI Disposition. This BAA shall remain in effect until all PHI received from, or created or received by, Business Associate on behalf of Covered Entity is returned to Covered Entity or destroyed in accordance with Section 13(d).
 - b. Material Breach. Upon either Party's knowledge of a material breach of this BAA by the other Party, the non-breaching Party must (i) provide an opportunity for the breaching Party to cure the breach or end the violation, and, if the breaching Party does not cure the breach or

end the violation within the time specified by the non-breaching Party, the non-breaching Party shall terminate this BAA and any underlying agreements that give rise to the business associate relationship described in this BAA ("Underlying Agreements"); or (ii) immediately terminate this BAA and any Underlying Agreements.

- c. Underlying Agreement. This BAA shall terminate simultaneously without additional notice upon the termination of any Underlying Agreement related to the Services or, if there is no Underlying Agreement, upon termination of the Services.
- d. Effect of Termination. Upon termination of this BAA for any reason, Business Associate agrees either to return to Covered Entity or to destroy all PHI received from or created or received by Business Associate on behalf of Covered Entity that is in the possession or control of Business Associate or its Subcontractors. If it is not feasible to return or destroy the information, Business Associate shall continue to comply with the terms in this BAA with respect to such PHI and shall comply with other applicable state or federal law.

14. Miscellaneous.

- a. Third-Party Beneficiaries. There are no third-party beneficiaries to this BAA. Business Associate's obligations are to the Covered Entity only.
- b. Counterparts. This BAA may be executed in counterparts, by manual, electronic, or facsimile signature, each of which will be deemed an original and all of which together will constitute one and the same instrument.
- c. Interpretation. Any ambiguity herein must be resolved in favor of a meaning that permits both Covered Entity and Business Associate to comply with Applicable Privacy Laws, consistent with the Terms of Services.