**HIPAA Business Associate Agreement**

This Business Associate Agreement (“Agreement”) is effective as of [INSERT DATE] between [INSERT NAME OF BUSINESS ASSOCIATE], a [INSERT TYPE OF BUSINESS] with its principal place of business at [INSERT STREET ADDRESS, CITY, STATE, ZIP CODE] (“Business Associate”) and [INSERT NAME OF PRACTICE PLAN] (“Covered Entity”), a New York not-for-profit corporation with its principal place of business at [INSERT STREET ADDRESS], Buffalo, New York [INSERT ZIP CODE].

**RECITALS**

1. The Parties have entered into one or more agreements entitled\_\_\_\_\_\_\_\_\_ and dated \_\_\_\_\_\_\_\_\_ in addition to any other agreements between the parties hereto (the “Services Agreement” or “Services Agreements”). Performance of the Services Agreement may involve Protected Health Information (“PHI”) (as defined in 45 CFR § 164.501) that is subject to the federal privacy and security regulations issued pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the regulations promulgated thereunder by the United States Department of Health and Human Services (“HHS”), codified at 45 CFR Parts 160 and 164 (commonly known as the Privacy, Security and Data Breach Notification & Enforcement Rules), (collectively referred to herein as the “HIPAA Rules”). The purpose of this Agreement is to set forth the obligations of the Parties with respect to such PHI.

II. Covered Entity is required to comply with the HIPAA Rules and enter into this Agreement to obtain satisfactory assurances that Business Associate will appropriately safeguard all PHI disclosed, created or received by Business Associate on behalf of Covered Entity.

III. Covered Entity desires to engage Business Associate to perform certain functions for, or on behalf of, Covered Entity involving the disclosure of PHI by Covered Entity to Business Associate, or the creation or use of PHI by Business Associate on behalf of Covered Entity, and Business Associate desires to perform such functions.

In consideration of the obligations under the Services Agreement, the mutual promises below and the exchange of information pursuant to this Agreement and in order to comply with all legal requirements for the protection of this information, the parties therefore agree as follows:

1. Definitions; Interpretation:

Except as otherwise defined herein, any and all initially capitalized terms in this Agreement shall have the definitions set forth in the HIPAA Rules and the HITECH Act. In the event of any inconsistency between the provisions of this Agreement, the Services Agreement, and the requirements of the HIPAA Rules, the HIPAA Rules shall control. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA Rules. All references to the HIPAA Rules are deemed to include all amendments to such rules contained in the HITECH Act and its implementing regulations, and any subsequently adopted amendments or regulations, as are applicable to this Agreement.

B. Obligations of Business Associate:

1. Relationship of Parties. In providing these services, Business Associate will be acting as an independent contractor and not as an employee or agent of Covered Entity. Covered Entity shall have no authority, express or implied, to commit or obligate Business Associate in any manner whatsoever. Business Associate will ensure that its employees and agents are aware of and agree to the same restrictions and conditions that apply to Business Associate with respect to PHI.
2. Permitted Use or Disclosure of PHI and Other Personal Information. Business Associate shall not use or disclose PHI other than as permitted or required in the Service Agreement and as set forth in Exhibit A to the Agreement or as required by law and shall also comply with applicable state law and regulations governing privacy, security and breach notification requirements related to personal information (“State Laws”).
3. Safeguards. Business Associate shall use appropriate administrative, physical and technical safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Agreement.
4. Privacy Rule. Business Associate will comply with all applicable requirements of the Privacy Rule.
5. Notice to Covered Entity. Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for in the Agreement, any Security Incident involving electronic PHI, and any Breach of Unsecured PHI as required at 45 CFR 164.410. Such report shall be provided promptly and without unreasonable delay, but no later than five days after Business Associate first learns of the unauthorized use or disclosure, Security Incident or Breach.
   1. Covered Entity shall be responsible for providing notification to individuals whose unsecured PHI has been disclosed, as well as the Secretary and the media, as required by HIPAA Rules. All notification costs will be paid for by Business Associate if the unauthorized use or the disclosure or breach is caused by Business Associate.
   2. The parties agree that this section satisfies any notices necessary by Business Associate to Covered Entity of the ongoing existence and occurrence of unsuccessful Security Incidents for which no additional notice to Covered Entity shall be required. For purposes of this Agreement, such unsuccessful Security Incidents include, without limitation, activity such as pings and other broadcast attacks on Business Associate’s firewall, port scans, unsuccessful log-on attempts, denial of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of Electronic PHI.
   3. Business Associate shall mitigate, to the extent practicable, the harmful effect caused by the unauthorized use or disclosure, Security Incident or Breach and provide notice of the mitigation efforts to Covered Entity.
6. Affiliates, Agents, Subsidiaries and Subcontractors. Business Associate agrees to ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information, in accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2).
7. Access to PHI. Business Associate will make PHI available within a reasonable amount of time of receipt of a request from Covered Entity or Individual to access such PHI. Business Associate shall make available such PHI to the extent required for Covered Entity’s compliance with its obligations under 45 CFR §164.524. If Business Associate receives a request from an Individual for access to PHI, Business Associate immediately shall forward such request to Covered Entity. Covered Entity shall be solely responsible for determining the scope of PHI and Designated Record Set with respect to each request by an Individual for access to PHI. If Business Associate maintains PHI in a Designated Record Set on behalf of Covered Entity, Business Associate shall permit any Individual, upon notice by Covered Entity, to access and obtain copies of the Individual’s PHI in accordance with 45 CFR Section 164.524. Business Associate shall make the PHI available in the format requested (electronic or hard copy) by the Individual and approved by Covered Entity, unless the PHI is not readily producible in such format, in which case the PHI shall be produced in hard copy format. Business Associate may not charge the Individual any fees for such access to PHI. Covered Entity shall reimburse Business Associate a portion of the fee charged by Covered Entity to the Individual that is proportional to the amount of PHI produced by Business Associate in relation to the amount of PHI produced by Covered Entity.
8. Amendment of PHI. To the extent that Business Associate possesses PHI, and within a reasonable amount of time of receipt of a request from Covered Entity or Individual, Business Associate shall make any amendment(s) to such PHI as directed or agreed to by the Covered Entity pursuant to 45 CFR § 164.526, or take other measures as necessary to satisfy Covered Entity’s obligations under 45 CFR § 164.526. Within five (5) business days following Business associate’s amendment of PHI, as directed by Covered Entity, Business Associate shall provide written notice to Covered Entity confirming that Business Associate has made the amendments to PHI as directed by Covered Entity and containing any other information as may be necessary for Covered Entity to provide adequate notice to the individual in accordance with 45 CFR § 164.526.
9. Disclosure Accounting. Business Associate shall document and make available such disclosures of PHI 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 CFR §164.528 and HITECH Act § 13405 (c) (3). The notice by Business Associate to Covered Entity of the disclosure shall include the name of the individual and Covered Entity affiliation to whom the PHI was disclosed and the date of the disclosure. Business Associate shall maintain a record of each such disclosure, including the date of the disclosure, the name and, if available, the address of the recipient of the PHI, a brief description of the PHI disclosed and a brief description of the purpose of the disclosure. Business Associate shall maintain this record for a period of six (6) years and make available to Covered Entity upon request in an electronic format so that Covered Entity may meet its disclosure accounting obligations under 45 CFR § 164.528.
10. Compliance with Covered Entity Obligations. To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, Business Associate shall comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).
11. Availability of Compliance 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 Department of Health and Human Services (the “Secretary”) for purposes determining Covered Entity’s compliance with the HIPAA laws and regulations. Upon reasonable notice to Business Associate and during Business Associate’s normal business hours, Business Associate shall make such internal practices, books and records available to Covered Entity to inspect for purposes of determining compliance with this Agreement. Additionally, Business Associate shall be subject to audits by the Secretary to ensure they comply with Subtitle D (Privacy) of Pub.L. 111-5 as well as 45 CFR 164 subparts C and E.
12. Ownership of Information. All PHI shall be deemed owned by the Covered Entity unless otherwise agreed in writing. During the term of this Agreement, Business Associate and any authorized sub-Business Associates shall have the right to use the PHI solely for the purposes of this Agreement. Business Associate and its agents shall not have the right to de-identify the PHI unless agreed to in writing by the Covered Entity.
13. Sale of PHI. Unless approved by Covered Entity, consistent with the exceptions set forth in Pub.L. 111-5 § 13405(d)(2), Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI of an individual unless Covered Entity has obtained from the Individual a valid authorization that includes a specification of whether the PHI can be further exchanged for remuneration by the entity receiving the PHI of that individual.
14. Marketing. Unless approved in writing, in advance, by Covered Entity, Business Associate shall not directly or indirectly perform marketing to Covered Entity patients using PHI that was either provided by Covered Entity, or created or otherwise acquired by Business Associate on behalf of Covered Entity.
15. Restrictions of Certain Disclosures. Business Associate shall comply with any restrictions on certain disclosures of PHI to which Covered Entity has agreed and communicated to Business Associate or which are required by HITECH.

C. Permitted Use and Disclosure of PHI:

1. Business Associate may only use or disclose PHI:
   1. As necessary to perform its obligations in the Services Agreement or functions as set forth in Exhibit A to this Agreement;
   2. As required by law.
   3. To Create de-identified information consistent with the standards of 45 CFR Sec. 164.512(a)-(c).
   4. Business Associate agrees to only disclose the minimum necessary PHI in performing its obligations under the Services Agreement.
2. Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity, except for the specific uses and disclosures set forth below:
   1. For the proper management and administration of Business Associate or to carry out its legal responsibilities;
   2. For the proper management and administration of Business Associate or to carry out its legal responsibilities, provided, the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and will be used or further disclosed only as required by Law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
   3. Use PHI to provide data aggregation services to the extent specified in the Services Agreement.
   4. Business Associate agrees to only disclose the minimum necessary PHI in performing its obligations under the Services Agreement.

D. Covered Entity’s Obligations:

1. Notice of Change in Privacy Practices. Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity’s notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect Business Associate’s use or disclosure of PHI.
2. Notice of Change in Permissions. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an individual to use or disclose PHI, to the extent that such changes may affect Business Associate’s use or disclosure of PHI.
3. Notice of Change in Use. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect Business Associate’s use or disclosure of PHI.
4. Appropriate Requests. Covered Entity shall not request that Business Associate use or disclose PHI in any manner that would not be permissible under the Law and Regulations if done by Covered Entity.

E. Terms and Termination:

1. Term. This Agreement shall become effective on the effective date of the first Services Agreement, and shall terminate at the time of the termination or expiration of all Services Agreements.
2. Termination Without Cause. Either party to this Agreement may terminate the Agreement upon provision of thirty (30) days prior written notice.
3. Termination With Cause. Either party may terminate this Agreement if the other has a receiver or trustee appointed for any or all of its property, becomes insolvent or otherwise is unable to pay its debts as they mature, makes an assignment for benefit of creditors, becomes subject to bankruptcy proceedings, or is dissolved or liquidated.
4. Termination for Breach. If Covered Entity reasonably determines that Business Associate has materially breached this Agreement, Covered Entity shall:
   1. Provide Business Associate with ten days written notice of the alleged material breach and an opportunity to cure the breach, immediately after which time this Agreement and the Services Agreement shall be automatically terminated if the breach is not cured; or
   2. Immediately terminate this Agreement and the Services Agreement if cure is not possible; or
   3. Take such action as may be allowed or required by the HIPAA Rules if neither termination nor cure is feasible.
5. Termination for Change in Law. If a change in law causes the performance of the Agreement to violate the law, Business Associate and/or Covered Entity shall terminate this Agreement if cure is not possible, or reasonably renegotiate the terms of this Agreement to comply with the change.
6. Effects of Termination: Disposal of PHI.
   1. Except as provided in paragraph b, below, upon termination of this Agreement for any reason, Business Associate shall return or destroy, at Covered Entity’s option, all PHI.  Business Associate shall insure compliance with this requirement by its subcontractors, if any.  Any such destruction shall comply with the applicable guidance of HHS in effect at the time of such destruction and Business Associate shall provide to Covered Entity a certification attesting to such compliance.
   2. Should Business Associate conclude that returning or destroying any PHI is not feasible, Business Associate shall immediately notify Covered entity in writing of the circumstances upon which it bases this conclusion.  Upon Covered Entity’s written concurrence that such return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI, and shall limit its further uses and disclosures to those purposes that necessitate Business Associate continuing to maintain this PHI.  The obligation of Business Associate under this provision shall survive termination of this Agreement, shall continue for as long as Business Associate maintains the PHI, and shall continue to bind Business Associate, its agents, contractors, successors and assigns, for however long the PHI is held by any of them.
   3. Mitigating Effects of Termination. In the event of termination of this Agreement, the parties agree to work together to effectuate a smooth transition for both parties and continuous protection of the PHI disclosed to or maintained by Business Associate.
   4. Survival. Business Associate’s obligations under this section survive the termination of the Agreement or Services Agreements.

F. Miscellaneous:

1. Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect of the effective date of the Agreement or as amended in the future.
2. Amendments. The Agreement may not be modified, nor shall any provision hereof be waived or amended expect in a writing duly signed by authorized representatives of the Parties. The Parties shall amend this Agreement from time to time as is necessary to achieve and maintain compliance with the requirements of the HIPAA Rules and any other applicable law.
3. Interpretation. Any ambiguity in this Agreement shall be resolved to permit the Parties to comply with the requirements of the HIPAA Rules and any other applicable law.
4. Choice of Law and Venue. This Agreement shall be governed by the laws of the State of New York without regard to conflict of laws principles thereof and any disputes involving this Agreement shall be exclusively venued in the New York State and Federal courts located in Erie County, New York.
5. Business Associate’s Compliance with HIPAA. Covered Entity makes no warranty or representation that compliance by Business Associate with this Agreement, HIPAA or the HIPAA regulations will be adequate or satisfactory for Business Associate’s own purposes or that any information in Business Associate’s possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.
6. Notices. Any notice required to be given pursuant to the terms and provisions of this Agreement shall be in writing and may be either personally delivered or sent by registered or certified mail in the United States Postal Services, return receipt requested, postage prepaid, addressed to each party at the addresses listed above or to such other addresses as the parties may hereinafter designate in writing.
7. Irreparable Harm. Any breach of the Agreement by Business Associate may cause irreparable harm to the Covered Entity. Therefore, Covered Entity may seek any legal remedy, including an injunction or specific performance for such harm without bond, security or necessity of demonstrating actual damages.
8. Indemnification. Business Associate shall defend, indemnify and hold harmless Covered Entity, its owners, employees and representatives, for any losses, fines, penalties, costs or damages incurred as a result of Business Associate’s breach of any provision of this Agreement or violation of any State Laws.
9. No Assignment. Neither party may assign its respective rights and obligations under this Agreement without the prior written consent of the other Party.
10. No Waiver. No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of any continuing or other liabilities or obligations, nor shall they prohibit enforcement of any liabilities or obligations on any other occasions.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement to be effective as of the date first written above.

COVERED ENTITY

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name:

Title:

BUSINESS ASSOCIATE

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name:

Title:

Exhibit A