



## HIPAA/HITECH BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT is made as of the day of **date** by and between Anderson Center for Autism with a primary business address of 4885 Route 9, Staatsburg, NY 12580 ("Covered Entity") and **BA** with a primary business address of **BA Address** ("Business Associate").

### RECITALS:

WHEREAS, the Covered Entity seeks to utilize the services of the Business Associate to provides services which involve use of Protected Health Information ("PHI").

WHEREAS, the parties desire to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Final Rule for Standards for Privacy of Individually Identifiable Health Information adopted by the United States Department of Health and Human Services ("HHS") and codified at 45 C.F.R. part 160 and part 164, subparts A & E (the "Privacy Rule"), the HIPAA Security Rule (the "Security Rule"), codified at 45 C.F.R. Part 164 Subpart C, and Subtitle D and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), including C.F.R. Sections 164.308, 164.310, 164.312, 164.316, and 164.402.

NOW THEREFORE, the parties to this Agreement hereby agree as follows:

- 1. Definitions.** Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule, the Security Rule, and HITECH, including 45 C.F.R. §§ 160.103, 164.103, 164.304, 164.402, 164.501, 164.502, 164.504, and Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules.
- 2. Obligations and Activities of Business Associate.**
  - a. Business Associate agrees to not use or further disclose PHI other than as permitted or required by this Agreement, as required by or permitted by law, provided the use or disclosure would also be permissible by law if made by the Covered Entity.
  - b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement. Business Associate agrees to implement administrative safeguards, physical safeguards and technical safeguards ("safeguards") that reasonably and appropriately protect the confidentiality, integrity and availability of PHI as required by the Security Rule, including those safeguards required pursuant to 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316, in the same manner that those requirements apply to the Covered Entity pursuant to 45 C.F.R. § 164.504.

- c. Business Associate agrees to 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 the requirements of this Agreement, or of any security incident of which it becomes aware.
- d. Business Associate agrees to report to the Covered Entity any use or disclosure of PHI not provided for by this Agreement, including breaches of unsecured PHI as required by 45 C.F.R. § 164.410; and any security incident of which it becomes aware.
- e. Business Associate agrees to ensure that any agent, including a subcontractor or vendor, to whom it provides PHI received from or created or received by Business Associate on behalf of the Covered Entity agrees to substantially similar restrictions and conditions that apply through this Agreement to Business Associate with respect to that information through a contractual arrangement that complies with 45 C.F.R. § 164.314.
- f. Business Associate agrees to provide paper or electronic access to PHI to the Covered Entity or as directed by the Covered Entity to an individual in order to meet the requirements under 45 C.F.R. § 164.524.
- g. Business Associate agrees to make any amendment(s) to PHI as directed in the time and manner by the Covered Entity or individual pursuant to 45 C.F.R. § 164.526.
- h. Business Associates agrees to make internal practices, books and records relating to the use and disclosure of PHI received from, created or received by the Business Associate on behalf of the Covered Entity available to the Secretary in a time and manner designated by the Secretary for the purposes of the Secretary determining the Covered Entity's compliance with the Privacy Rule and Security Rule.
- i. Business Associate agrees to document disclosures of PHI and the information related to the disclosures that would be required for the 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.
- j. Business Associate agrees to provide to the Covered Entity or an Individual, in a time and manner designated by the Covered Entity, information collected in accordance with this Agreement, to permit the Covered Entity to respond to a request by an individual for an accounting of disclosures for PHI in accordance with 45 C.F.R. § 164.528.
- k. If Business Associate discloses Unsecured Protected Health Information (as defined in 45 C.F.R. § 164.402), it shall promptly notify the Covered Entity of the breach. The notice shall include: (a) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (b) a description of the types of Unsecured Protected Health Information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); and (c) a brief description of what the Business Associate is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.
- l. Business Associate agrees that it will not receive remuneration directly or indirectly in exchange for PHI without authorization unless an exception under 13405(d) of the HITECH Act applies.
- m. Business Associate agrees that it will not receive remuneration for certain communications that fall within the exceptions to the definition of Marketing under 45

C.F.R. § 164.501 unless permitted by the HITECH Act.

- n. Business Associate agrees that it will not use or disclose genetic information for underwriting purposes, as that term is defined in 45 C.F.R. § 164.502.
- o. Business Associate hereby agrees to comply with state laws applicable to PHI and personal information of individuals' information it receives from the Covered Entity during the term of the Agreement.
  - 1. Business Associate agrees to:
    - a) Implement and maintain appropriate physical, technical, and administrative security measures for the protection of personal information as required by New York State law, but not limited to:
      - i. Encrypting all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly;
      - ii. Prohibiting the transfer of personal information to any portable device that has not been approved in advance; and
      - iii. Encrypting any personal information to be transferred to a portable device.
    - b) Implement and maintain a Written Information Security Program as required by New York State law.
  - 2. The safeguards set forth in this Agreement shall apply equally to ePHI, PHI, and confidential and "personal information." Personal information is defined by any applicable law or regulation and means any information about an individual maintained by any agency, company or organization, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information; it also includes combinations of information such as an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password, that would permit access to a resident's financial account; provided it is also information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context; however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

### **3. Permitted Uses and Disclosures by Business Associate.**

- a. Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform one or more functions for, or on behalf of, the Covered Entity provided that the use or disclosure would not violate the Privacy Rule if done by the Covered Entity or the minimum necessary policies and procedures of the Covered Entity required

by 45 C.F.R. § 164.514(d).

- b. Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- c. Except as otherwise limited in this Agreement, Business Associate may disclose PHI provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential 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 the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- d. Except as otherwise limited in this Agreement, Business Associate may use PHI to provide Data Aggregation services to the Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).
- e. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).

#### **4. Obligations of the Covered Entity**

- a. The Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of the Covered Entity in accordance with 45 C.F.R. § 164.520, to the extent that the limitation may affect Business Associate's use or disclosure of PHI.
- b. The 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 the changes may affect Business Associate's use or disclosure of PHI.
- c. The Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that the restriction may affect Business Associate's use or disclosure of PHI. Otherwise, Covered Entity agrees that it will not furnish or impose by arrangements with third parties or other covered entities or Business Associates special limits or restrictions to the uses and disclosures of its PHI that may impact in any manner the use and disclosure of PHI by Business Associate.

#### **5. Permissible Requests by the Covered Entity**

- a. The Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity, provided that, to the extent permitted by the Service Arrangement, Business Associate may use or disclose PHI for Business Associate's Data Aggregation activities or proper management and administrative activities.

#### **6. Compliance with Electronic Transactions Rule**

- a. If Business Associate conducts in whole or part Electronic Transactions on behalf of the Covered Entity for which HHS has established standards, Business Associate will comply, and will require any subcontractor or agent it involves with the conduct of Electronic Transactions to comply, with each applicable requirement of the Electronic

Transactions Rule at 45 C.F.R. Part 162. Business Associate shall also comply with the National Provider Identifier requirements, if and to the extent applicable.

**7. Term and Termination.**

- a. The term of this Agreement shall begin as of the effective date of the Service Arrangement and shall terminate when all of the PHI provided by the Covered Entity to Business Associate, or created or received by Business Associate on behalf of the Covered Entity, is destroyed or returned to the Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to the information, in accordance with the termination provisions of this Section. Business Associate agrees that all provisions will remain in effect, and any updates shall be available at <http://www.andersoncenterforautism.org/compliance>. Business Associate remains responsible for knowledge of and compliance with all updates to this agreement.
- b. Upon either party's knowledge of a material breach by the other party, the non-breaching party shall either:
  - i. Provide an opportunity for the breaching party to cure the breach or end the violation and terminate this Agreement and the Service Arrangement if the breaching party does not cure the breach or end the violation within a reasonable time specified by the non-breaching party,
  - ii. Immediately terminate this Agreement and the Service Arrangement if the breaching party has breached a material term of this Agreement and cure is not possible, or
  - iii. If neither termination nor cure is feasible, the non-breaching party shall report the violation to the Secretary.
- c. Except as provided in paragraph (d) of this Section, upon any termination or expiration of this Agreement, Business Associate shall return or destroy all PHI received from the Covered Entity, or created or received by Business Associate on behalf of the Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI. Business Associate shall ensure that its subcontractors or vendors return or destroy any of Covered Entity's PHI received from Business Associate.
- d. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to the Covered Entity notification of the conditions that make return or destruction infeasible. Upon the Covered Entity's written agreement that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to the PHI and limit further uses and disclosures of the PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains the PHI.

**8. Miscellaneous.**

- a. A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.
- b. The Parties agree to take actions that are necessary to amend this Agreement from

time to time as is necessary for the Covered Entity to comply with the requirements of HIPAA, the Privacy and Security Rules and HITECH.

- c. The respective rights and obligations of Business Associate under Section 7 (c) and (d) of this Agreement shall survive the termination of this Agreement.
- d. Any ambiguity in this Agreement shall be resolved to permit the Covered Entity to comply with HIPAA and HITECH.
- e. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer upon any person other than the Covered Entity, Business Associate and their respective successors and assigns, any rights, remedies, obligations or liabilities whatsoever.
- f. Modification of the terms of this Agreement shall not be effective or binding upon the parties unless and until the modification is committed to writing and executed by the parties hereto.
- g. This Agreement shall be binding upon the parties hereto, and their respective legal representatives, trustees, receivers, successors and permitted assigns.
- h. Should any provision of this Agreement be found unenforceable, it shall be deemed severable and the balance of the Agreement shall continue in full force and effect as if the unenforceable provision had never been made a part hereof.
- i. This Agreement and the rights and obligations of the parties hereunder shall in all respects be governed by, and construed in accordance with, the laws of the State of New York, including all matters of constructions, validity, and performance.
- j. All notices and communications required or permitted to be given hereunder shall be sent by certified or regular mail, addressed to the other party at its respective address as shown on the signature page, or at another address that the party shall from time to time designate in writing to the other party, and shall be effective from the date of mailing.
- k. This Agreement, including the portions that are incorporated by reference herein, constitutes the entire agreement by, between and among the parties, and the parties acknowledge by their signature hereto that they do not rely upon any representations or undertakings by any person or party, past or future, not expressly set forth in writing herein.

IN WITNESS WHEREOF, the undersigned have executed this Agreement as of the date first set forth above.

**Anderson Center for Autism**

**Business Associate.**

By: \_\_\_\_\_  
(Signature)

By: \_\_\_\_\_  
(Signature)

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Print Name