
# HIPAA BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("**Agreement**"), is between Birch Family Services, Inc., a New York not-for-profit corporation ("**Covered Entity**") and _____ ("**Business Associate**") (each a "**Party**" and collectively, the "**Parties**").

**WHEREAS**, Business Associate provides services to Covered Entity that may involve or require the use or disclosure of Protected Health Information (as defined herein); and

**WHEREAS**, Covered Entity is considered a "Covered Entity" and, to the extent Business Associate's services involve the use or disclosure of Protected Health Information, Business Associate is considered a "Business Associate," as such terms are defined under HIPAA and the regulations promulgated thereunder (45 C.F.R. Parts 160, 162 and 164, as amended from time to time), as amended by HITECH and the regulations promulgated thereunder (collectively, the "**Privacy and Security Laws**");

**NOW THEREFORE**, Covered Entity and Business Associate agree as follows:

## 1. Definitions.

(a) "**Breach**" means the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of PHI, subject to the exceptions provided in 45 C.F.R. 164.402(1)(i)-(iii). For purposes of this definition, any acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule shall be presumed to be a Breach unless it is demonstrated, through a risk assessment, that there is a low probability that the PHI has been compromised.

(b) "**Breach Notification Rule**" means the rules found in 45 C.F.R. Part 160 and Subparts A and D of 45 C.F.R. Part 164, as amended.

(c) "**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996, as amended.

(d) "**HITECH**" means Title XII, Subtitle D of the Health Information Technology for Economic and Clinical Health Act, codified at 42 USC §§ 17921-17954.

(e) "**Individual**" shall have the same meaning as the term "individual" in 45 C.F.R. 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. 164.502(g).

(f) "**Privacy Rule**" means the rules found in 45 C.F.R. Part 160 and Subparts A and E of 45 C.F.R. Part 164, as amended.

(g) "**Protected Health Information**" or "**PHI**" means individually identifiable health information as defined in 45 C.F.R. 160.103, limited to the information received by Business Associate from Covered Entity or created or received by Business Associate on behalf of Covered Entity, including, but not limited to electronic PHI.

(h) "**Regulations**" means the Privacy Rule, the Security Rule, and the Breach Notification Rule, collectively.

(i) "**Required By Law**" shall have the same meaning as the term "required by law" in 45 C.F.R. 164.103.

(j) "**Secretary**" means the Secretary of the Department of Health and Human Services or his/her designee.

(k) "**Security Rule**" means the rules found in 45 C.F.R. Part 160 and Subparts A and C of 45 C.F.R. Part 164, as amended.

(l) "**Unsecured PHI**" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of HITECH.

(m) "**Unsuccessful Security Incident**" means, without limitation, activity such as pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized access to PHI, or any use or disclosure of PHI.

(n) Unless defined herein, all other capitalized terms in this Agreement have the meanings given to them in the Regulations, HIPAA, and HITECH.

**2. Permitted Uses and Disclosures.**

(a) General Prohibition. All uses or disclosures of PHI not authorized by this Agreement or Required by Law are prohibited.

(b) Internal Use and Disclosure to Employees. Business Associate may use or disclose PHI to its employees only as necessary to perform functions, activities, or services for, or on behalf of, Covered Entity and for which Covered Entity has engaged Business Associate, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity, or otherwise violate this Agreement.

(c) Disclosure to Third Parties. Business Associate may disclose PHI to third parties, including its authorized subcontractors, only as necessary to perform functions, activities, or services for, or on behalf of, Covered Entity and for which Covered Entity has engaged Business Associate, provided that:

(i) the disclosure is Required by Law; or

(ii) Business Associate enters into an agreement with each third party that will have access to PHI that is received from, or is created or received by, Business Associate on behalf of Covered Entity that: (*x*) the PHI will remain confidential and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the third party; (*y*) the third party will notify Business Associate of any Reportable Event (as defined herein); and (*z*) the third party agrees in writing to be bound by the same restrictions, terms, and conditions that apply to Business Associate under this Agreement.

(d) Proper Management and Administration. Subject to any other limitations in this Agreement, Business Associate may use PHI as necessary for the proper management and administration of Business Associate or to carry out any present or future legal responsibilities of Business Associate, provided such uses are permitted under the Privacy Rule.

(e) Minimum Necessary. Business Associate shall only request, use, or disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use, or disclosure. Business Associate shall limit requests, uses, and disclosure of PHI, to the extent practicable, to a Limited Data Set (as defined at 45 C.F.R. 164.514[e]), and in all other cases subject to the requirements of 45 C.F.R. 164.502(b), to the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure.

**3. Nondisclosure.**

(a) Disclosures Required by Law. Business Associate shall not, without the prior written consent of Covered Entity, disclose any PHI on the basis that such disclosure is Required by Law without notifying Covered Entity so that Covered Entity shall first have an opportunity to object to the disclosure and to seek appropriate relief. If Covered Entity objects to such disclosure, Business Associate shall refrain from disclosing the PHI until Covered Entity has exhausted all available remedies. Business Associate shall require that persons or entities receiving PHI in accordance with Section 2(c) hereof provide Covered Entity with similar notice and opportunity to object before disclosing PHI on the basis that such disclosure is Required by Law.

(b) Additional Restrictions. If Covered Entity notifies Business Associate that Covered Entity has agreed to be bound by additional restrictions on the use or disclosure of PHI pursuant to the Privacy Rule, Business Associate shall be bound by such additional restrictions and shall not disclose PHI in violation of such additional restrictions.

**4. Safeguards, Reporting, and Mitigation.**

(a) Privacy Safeguards. Business Associate shall comply with the Privacy Rule, and shall use all appropriate safeguards to prevent any use or disclosure of PHI other than as permitted by the terms of this Agreement.

(b) Security Safeguards for Electronic PHI. Business Associate shall comply with the Security Rule, including the requirements of 45 C.F.R. 164.308 (administrative safeguards), 45 C.F.R. 164.310 (physical safeguards), 45 C.F.R. 164.312 (technical safeguards) and 45 C.F.R. 164.316 (policies and procedures and documentation requirements). Pursuant to the foregoing requirements, Business Associate shall implement 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.

(c) Reporting Requirements.

(i) Business Associate shall report to Covered Entity any Breach of Unsecured PHI and any other use or disclosure of PHI not permitted by this Agreement.

(ii) Business Associate shall also report to Covered Entity any Security Incident (as defined by the Security Rule) of which it becomes aware; provided however, the Parties agree that this section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence or attempts of Unsuccessful Security Incidents for which no additional notice or report to Covered Entity shall be required.

(iii) As soon as practical but no later than five (5) business days after Business Associate learns of the occurrence of any non-permitted use or disclosure of PHI, Security Incident or Breach of Unsecured PHI (collectively, a "**Reportable Event**"), Business Associate shall notify the designated Privacy Officer of Covered Entity of such occurrence.

(iv) As soon as practical but no later than five (5) business days of Business Associate notifying Covered Entity of any Reportable Event, Business Associate shall provide a written report to Covered Entity, unless despite all reasonable efforts by Business Associate to obtain the information required in subparagraphs 4(c)(iv)(a)-(g) below, circumstances beyond the control of Business Associate necessitate additional time. Under such circumstances Business Associate shall provide to Covered Entity the information contained in subparagraphs 4(c)(iv)(a)-(g) below as soon as possible and without unreasonable delay, but in no event later than thirty (30) calendar days from the date of discovery of the Reportable Event. Business Associate's report shall:

(a) Identify the nature of the Reportable Event;

(b) Identify the date of the Reportable Event and the date of the discovery of such event, if known;
(c) Identify the PHI used or disclosed and the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during the Reportable Event;
(d) Identify who made the non-permitted use or received the non-permitted disclosure;
(e) Identify what corrective action Business Associate took or will take to prevent future similar Reportable Events;
(f) Identify what Business Associate did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; and
(g) Provide such other information, including a written report, as Covered Entity may reasonably request.

(v) As between Covered Entity and Business Associate, Covered Entity shall have final authority to determine whether any Reportable Event is a Breach of Unsecured PHI, whether notification requirements under the Breach Notification Rule have been triggered, and the necessity for and content of any required notifications. Business Associate shall cooperate fully to assist Covered Entity in identifying individuals potentially affected by a Breach of Unsecured PHI, conducting the risk assessment required by the Breach Notification Rule, and providing any notifications required by the Regulations. To the extent that the Reportable Event resulted from acts or omissions of Business Associate or its agents, Business Associate shall be responsible for all costs reasonably incurred by Covered Entity or Business Associate as a result of such Reportable Event.

(d) Mitigation. Business Associate shall have procedures in place to mitigate, and shall cooperate with Covered Entity to mitigate, to the maximum extent practicable, any harm or damage resulting from the use or disclosure of PHI in violation of this Agreement or in violation of the Privacy Rule.

**5. Access, Amendment, and Accounting of PHI.**

(a) Access to PHI. Within ten (10) business days of a request by Covered Entity for access to PHI about an individual contained in a Designated Record Set, Business Associate will make available to Covered Entity such PHI for so long as such information is maintained in the Designated Record Set. Business Associate will promptly forward to Covered Entity any direct requests for access to PHI. Covered Entity will be solely responsible for approving or disapproving any such request for access to the PHI, and Business Associate will comply with Covered Entity's directions regarding such requests. Notwithstanding the above, if Business Associate or its agents or subcontractors uses or maintains PHI in an electronic health record then within ten (10) days of receipt of a request from Covered Entity, Business Associate shall make a copy of such PHI available to Covered Entity in an electronic format in order to enable Covered Entity to fulfill its obligations under 45 C.F.R. 164.524(c)(2)(ii).

(b) Availability of PHI for Amendment. Within ten (10) business days of receipt of a request from Covered Entity for the amendment of an individual's PHI or a record regarding an individual contained in a Designated Record Set (for so long as the PHI is maintained in the Designated Record Set), Business Associate will provide such information to Covered Entity for amendment and incorporate any such amendments in the PHI, as required by 45 C.F.R. 164.526.

(c) Accounting of Disclosures. Business Associate agrees to document disclosures of PHI and such 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. Within ten (10) business days of notice by Covered Entity to Business Associate that Covered Entity has received a request for an accounting of disclosures of PHI regarding an individual, Business Associate will make available to Covered Entity such information as is in Business Associate's possession and is required for Covered Entity to make the accounting required by 45 C.F.R. 164.528. In the event that the request for an accounting is delivered directly to Business Associate, Business Associate shall within two (2) days of such request forward

it to Covered Entity in writing. It shall be Covered Entity's responsibility to prepare and deliver any accounting requested. Business Associate shall not disclose any PHI except as permitted by this Agreement. Business Associate shall continue to maintain the information required under this paragraph for a period of six (6) years after the applicable disclosure.

(d) Availability of Books and Records. Business Associate will 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 United States Department of Health and Human Services for purposes of determining Covered Entity's and Business Associate's compliance with the Privacy and Security Laws.

**6. Additional Prohibitions and Restrictions.**

(a) Prohibition on Sale of PHI. Business Associate shall not sell PHI as prohibited by 45 C.F.R. 164.502(a)(5)(ii) and 45 C.F.R. 164.508(a)(4).

(b) Marketing. Business Associate shall not use or disclose PHI in connection with any Marketing (as defined by 45 C.F.R. 164.501) that is prohibited by 45 C.F.R. 164.508(a)(3).

(c) Fundraising. Business Associate shall not use or disclose PHI in connection with any written Fundraising communication that is prohibited by 45 C.F.R. 164.514(f).

(d) Confidential Communications. Business Associate shall, if directed by Covered Entity, use alternative means or alternative locations when communicating PHI to an Individual based on the Individual's request for confidential communications in accordance with 45 C.F.R. 164.522, including but not limited to complying with all requests for restrictions as required under 45 C.F.R. 164.522(a)(1)(iii) and (vi).

**7. Obligations of Covered Entity.**

(a) Notice of Limitations. Covered Entity will notify Business Associate of (i) any limitation(s) in Covered Entity's notice of privacy practices in accordance with 45 C.F.R. 164.520; (ii) any changes in, or revocation of, permission by an individual to use PHI; and (iii) any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. 164.522, to the extent that such limitation, change, revocation or restriction may affect Business Associate's use or disclosure of PHI.

(b) Permissible Requests by Covered Entity. Covered Entity will not request Business Associate to use or disclose PHI in any manner that is not be permissible under the Privacy Rule if done by Covered Entity.

**8. Term and Termination.**

(a) Term. This Agreement shall take effect upon the latest date on which this Agreement is signed by either party, and shall continue in effect until all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, until protections are extended to such information, in accordance with the termination provisions in this Section.

(b) Termination Upon Breach. In addition to any other remedies available to Covered Entity at law or in equity:

(i) Covered Entity may immediately terminate this Agreement and any agreement under which Business Associate's services have been engaged, if Covered Entity determines that Business Associate has breached a material term of this Agreement or has violated any provision of the Privacy and Security Laws.

(ii) Alternatively, Covered Entity may choose to provide Business Associate with written

notice of the existence of the material breach or violation and afford Business Associate an opportunity to cure the same upon mutually agreeable terms; provided, however, that Business Associate must cure the breach or violation to the satisfaction of Covered Entity not later than thirty (30) calendar days after Covered Entity gives such notice. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination this Agreement and any agreement under which Business Associate's services have been engaged.

(iii) Notwithstanding Section 8(b)(i) and (ii), if Business Associate's cure of the breach or violation is not successful within the time provided above, and termination of this Agreement is not feasible in Covered Entity's sole discretion, Covered Entity may report Business Associates' breach or violation to the Secretary of the United States Department of Health and Human Services, and Business Associate agrees that it shall not have or make any claim, whether at law, in equity, under this Agreement, or otherwise, against Covered Entity with respect to such report.

(iv) If Business Associate knows of a pattern of activity or practice of Covered Entity that constitutes a material breach or violation of Covered Entity's duties and obligations under either this Agreement or the Privacy and Security Laws, Business Associate shall provide an opportunity for Covered Entity to cure the material breach or violation; provided however, if Covered Entity does not cure the material breach or violation to Business Associate's satisfaction within thirty calendar days, Business Associate may terminate this Agreement, if feasible.

(c) Effect of Termination.

(i) Except as provided in paragraph 8(c)(ii) below, upon termination of this Agreement and/or any agreement under which Business Associate's services have been engaged, Business Associate shall either return to Covered Entity or destroy all existing PHI received or created from or on behalf of Covered Entity, including PHI in the possession of Business Associate's subcontractors or agents. Business Associate shall retain no copies of such PHI.

(ii) In the event that Business Associate determines it is not feasible to return or destroy PHI, Business Associate must notify Covered Entity of the conditions that make return or destruction infeasible and, in such event, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

**9. General.**

(a) Indemnification. Each Party shall indemnify and hold harmless the other Party and its officers, directors, employees, and agents from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees and court or proceeding costs, arising out of or in connection with any use or disclosure of PHI not permitted by this Agreement or by the Privacy Rule, or other breach of this Agreement or the Regulations by the indemnifying Party or any subcontractor, agent, or person under the indemnifying Party's control, including but not limited to any penalties or fines arising from violation of the Privacy and Security Laws and the reasonable cost to comply with the notification requirements pursuant to 45 C.F.R. 164.404, 45 C.F.R. 164.406 and 45 C.F.R. 164.408. The Parties acknowledge that in addition to the indemnification obligations hereunder, each Party shall be directly responsible for, and hold the other harmless against, any civil and/or criminal penalties arising from its violation of the Privacy and Security Laws. Each Party's obligations hereunder are expressly excluded from any provisions of any other agreements between the Parties that would otherwise limit the Party's liability.

(b) Survival of Obligations. The obligations of the Parties under this Agreement shall survive termination of Business Associate's services to Covered Entity and any agreement under which such services have been engaged.

(c) Equitable Remedies. Business Associate recognizes that irreparable injury will result to Covered Entity if Business Associate breaches any provision(s) of this Agreement. Business Associate agrees

that if it should engage, or directly cause any other person or entity to engage, in any act in violation of any provision hereof, that Covered Entity will be entitled, in addition to such other remedies, damages and relief as may be available under applicable law, to an injunction prohibiting Business Associate from engaging in any such act or specifically enforcing this Agreement, as the case may be. No failure or delay by Covered Entity in exercising any right, power or privilege under this Agreement shall operate as waiver thereof, nor shall any single or partial exercise thereof preclude any other or further exercise thereof.

(d) Regulatory References. A reference in this Agreement to a section in the Privacy and Security Laws means the section as in effect or as amended, and for which compliance is required.

(e) Notice Regarding Compelled Disclosure. If Business Associate is requested pursuant to, or believes it is required by, applicable law or regulation or by legal process to disclose any PHI, Business Associate will provide Covered Entity with prompt written notice of such request(s) to enable Covered Entity to control the response to such request(s) and, where appropriate, to seek an appropriate protective order or pursue other authorized procedures to challenge the attempt to compel disclosure. Business Associate will cooperate with Covered Entity in its efforts to challenge such compelled disclosure.

(f) Entire Agreement. This Agreement constitutes the entire agreement between the Parties on the subject matter of this Agreement, and supersedes all oral and written prior representations, agreements, and understandings relating to the subject matter, including any conflicting provisions of any prior or contemporaneous agreements between the Parties.

(g) Waiver and Amendment. No waiver of any breach of any provision of this Agreement shall constitute a waiver of any subsequent breach of the same or any other provisions of this Agreement. This Agreement may not be amended, modified, supplemented, or rescinded except by a writing signed by both Parties. Notwithstanding the forgoing, the Parties agree that this Agreement shall be deemed amended without requiring further action by either Party, as may be necessary from time to time for Covered Entity to comply with amendments, revisions, and additions to the Privacy and Security Laws.

(h) Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of this Agreement which can be given effect without the invalid provision shall continue in full force and effect and shall in no way be impaired or invalidated.

(i) Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy and Security Laws, and all other Federal and State laws.

(j) No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer upon any person other than Covered Entity, Business Associate and their respective successors and assigns, any rights, remedies, obligations or liabilities.

(k) No Creation of Service Term. Nothing in this Agreement shall be construed as giving Business Associate a right to provide or to continue to provide any services to Covered Entity other than as specifically provided in the agreement(s) between them.

| **COVERED ENTITY:**<br>**Birch Family Services, Inc.** | **BUSINESS ASSOCIATE** |
|---|---|
| By: _____ | By: _____ |
| Name: Matthew Sturiale, LCSW | Name: _____ |
| Title: Chief Executive Officer | Title: _____ |
| Date: _____ | Date: _____ |