Topic: Business Associates and Business Associate Agreements	**Department:** Entire Agency
Original effective date: 4/1/03	**Last revision date:** 2/23/22
Owner: VP for Quality and Compliance	**Frequency of reviews:** Annual
Internal/Regulatory Reference(s) (all that apply): 160.310; 164.410	
Related documents/Links: Business Associate Agreement	

Policy: It is the policy of The Arc of Monroe to ensure that people have opportunities for privacy and that business, administrative and support functions promote personal and organizational outcomes.

Additional Information: For the purposes of this procedure, a "business associate" is someone who, on behalf of The Arc, creates, receives, maintains or transmits PHI for a function or activity that is regulated by HIPAA law. This includes a number of things such as, but not limited to:

- Billing, or claims processing or administration
- Data analysis, processing or administration
- Utilization review
- Quality assurance
- Accounting services

Examples include:

- Health information organizations that provide data transmission services with respect to PHI
- A company we work with that stores and manages PHI for us, such as our electronic health record
- Someone that offers a personal record to one or more people we support on behalf of The Arc
- A subcontractor that creates, receives, maintains or transmits PHI on behalf of a business associate.

Business associates do not include:

- Another health care provider who also provides services to someone we support (such as a doctor that someone sees or someone's non-Arc residential provider)
- A government agency who is responsible for determining eligibility for, or enrollment in, a government health plan (such as Medicaid or Medicare)

The detailed responsibilities of the Business Associate are contained in the Business Associate Agreement (BAA) (See attached). The VP for Quality and Compliance has primary responsibility to ensure compliance with HIPAA law in regards to business associates and BAAs.

For the purposes of this procedure, "staff" includes employees, contractors, consultants, interns, students and volunteers.

"Protected health information or PHI" is defined as information about people we support that relates to their past, present or future mental or physical health and also identifies them in some way. In addition to more obvious things such as treatment plans, service documentation, clinical assessment, etc., the following are also considered PHI:

- Initials of someone we support. If you share initials, you are sharing PHI. Reducing a name to initials does not protect it under HIPAA law.
- Pictures of someone we support. This includes any photograph that will identify the person in some way. This may be the case even if their face isn't visible, but something distinctive about them is. It could also apply to pictures of the back of their head, side shots, other parts of their bodies that are distinctive, etc.
- Anything that describes someone in a way that makes it clear who you are talking about (such as a full physical description; or a combination of characteristics that are so unique as to effectively name the person). EXAMPLE: A short middle-aged woman with blazing red hair and right-side hemiparesis who goes to Henrietta Day Services.

This definition applies whether the information is written, spoken, signed, or in an electronic format – regardless of the language (e.g., English or any other language). You should presume that any information about people we support that you work with in your job is PHI and should be treated as such.

Procedure	
Task:	**Responsible party:**
General Guidelines	
1. Whenever The Arc enters into a contract with another company, an assessment will occur as to whether or not a BAA is necessary, based on the criteria above and in HIPAA law. The VP for Quality and Compliance should be consulted if there are any questions as to whether or not one is needed. There may also be instances where a BAA is required when other contracts are not.	Leadership
2. The VP for Quality and Compliance will assist as necessary in making this determination.	VP for Quality and Compliance
3. If the determination is that a BAA is appropriate, the leader will notify VP for Quality and Compliance (if not already informed).	Leadership
4. If the BA provides a BAA for us to sign as the covered entity (this should not happen, but it sometimes does), it should be forwarded to the VP for Quality and Compliance for review prior to signature. At the discretion of the VP for Quality and Compliance, this proposed BAA may be sent to legal counsel for their review and approval.	Leadership, VP for Quality and Compliance
5. Once approved or if using our own BAA, the leader will ensure that the BAA is sent out to the appropriate party at the business associate for review and signature.	Leadership

6. If the contractor proposes any changes to The Arc of Monroe's BAA, these requests will be sent to the VP for Quality and Compliance for review. They will contact legal counsel as appropriate for guidance.	Executive Assistant, VP for Quality and Compliance
7. Once an agreed-upon BAA has been returned by the contractor, the Executive Assistant will ensure that it is signed by the CFO.	Executive Assistant, CFO
8. Once signed, the Executive Assistant will maintain the original signed copy and will send a copy to the VP for Quality and Compliance. On this copy, the Executive Assistant will document the duration of the contract (dates) if applicable. This can be done by hand at the top of the copy. This will assist the VP for Quality and Compliance in managing existing BAAs. If the BAA is not tied to a specific contractual period, no date needs to be written.	Executive Assistant
9. The VP for Quality and Compliance will periodically review the list of BAAs and remove any for whom the contract period has expired and will not be renewed.	VP for Quality and Compliance
10. The VP for Quality and Compliance reserves the right to enact elements of the BAA to ensure that the business associate is in compliance with HIPAA law, consistent with the terms of the BAA.	VP for Quality and Compliance
11. In the event that the business associate experiences a breach involving Arc of Monroe PHI, the VP for Quality and Compliance will work with the business associate as appropriate and as outlined in the BAA. They may consult with legal counsel as appropriate.	VP for Quality and Compliance
12. If we receive a BAA as a business associate to another covered entity, the BAA should be forwarded to the VP for Quality and Compliance for review before signature.	Leadership; VPQC
13. Once approved, it should go to the CFO for signature.	VPQC; Leadership; CFO
Leadership responsibilities:	
1. Members of leadership are responsible for consulting with the VP for Quality and Compliance if/when there are questions as to whether a BAA is required.	Leadership
2. Members of leadership are responsible for ensuring that BAAs are sent out for review and signature, consistent with this procedure.	Leadership
VP for Quality and Compliance:	
1. Acts as the agency's Privacy Officer	VP for Quality and Compliance
2. Responsible for administering the agency's HIPAA privacy policies and procedures	VP for Quality and Compliance
3. Acts as a resource for staff and leadership in regards to proper implementation of the HIPAA privacy rule	VP for Quality and Compliance
4. Has ultimate responsibility for The Arc's compliance with business associate provisions.	VP for Quality and Compliance

Document revision record:

Revision Date	Release Date	Reason for change	Approver
10/24/11	10/24/11	Reasons for change not documented	P Dancer
8/5/15	8/5/15	Reasons for change not documented	P Dancer
12/31/18	12/31/18	Reasons for change not documented	P Dancer
1/29/21	1/29/21	Transfer to the new procedural format and fleshed out	P Dancer
2/23/22	3/4/22	Clarified the BAA implementation process and added a bullet about BAAs with Arc as the BA	ICC
2/8/24	3/18/24	Clarified that BA-proposed BAAs may be sent to legal counsel for review at discretion of VPQC	ICC

The Arc of Monroe

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT (the "Agreement") is made and entered into effective as of _____ between **The Arc of Monroe**, a human services agency providing services to people with intellectual and other developmental disabilities, and/or people meeting NYS DOH health home requirements, with a primary address of 2060 Brighton-Henrietta TL Road, Rochester, NY 14623 (the covered entity) and _____ with an address at _____ (the "BUSINESS ASSOCIATE"). This Business Associate Agreement replaces in its entirety, as of the date hereof, any existing Business Associate Agreement between the parties listed and incorporates requirements of the final HIPAA/HITECH Omnibus Rule.

As required by the Health Insurance Portability and Accountability Act of 1996, ("HIPAA") and the 2009 American Renewal and Revitalization Act, (ARRA) and the regulations promulgated thereunder (including the Health Information Technology for Economic and Clinical Health Act- "HITECH"), and in consideration for COVERED ENTITY engaging BUSINESS ASSOCIATE to provide Services and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, BUSINESS ASSOCIATE and COVERED ENTITY hereby agrees as follows:

1. Definitions

a. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 CFR Part 160 and Part 164 and ARRA §13401, §13402 and §13404, §13405 and any other applicable areas.
b. "BUSINESS ASSOCIATE" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103.
c. "COVERED ENTITY" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean The Arc of Monroe County.
d. Services" means those specific activities and/or functions for which COVERED ENTITY engages BUSINESS ASSOCIATE to perform for COVERED ENTITY or on COVERED ENTITY'S behalf. Such engagement(s) may be by written or oral agreement entered into before or after the date of this Agreement.
e. "Protected Health Information" means information received from, or created or received by BUSINESS ASSOCIATE on behalf of, COVERED ENTITY including demographic information collected from an Individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an Individual, which information identifies the Individual or with respect to which there is a reasonable basis upon which to believe that the information can be used to identify the Individual.

2. Permitted Uses and Disclosures

Except as otherwise limited in this Agreement, BUSINESS ASSOCIATE may:

a. Use or disclose Protected Health Information to perform Services provided that such use or disclosure would not violate HIPAA, ARRA or HITECH Privacy or Security Rules if done by COVERED ENTITY;
b. Use Protected Health Information for purposes of the proper management and administration of BUSINESS ASSOCIATE and to carry out BUSINESS ASSOCIATE'S legal responsibilities; and

c. Disclose Protected Health Information for purposes of the proper management and administration of BUSINESS ASSOCIATE and to carry out BUSINESS ASSOCIATE'S legal responsibilities if such disclosure is required by law or if BUSINESS ASSOCIATE obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person.

3. Obligations

As required by the HIPAA, ARRA and HITECH Regulations, BUSINESS ASSOCIATE agrees to:

a. Not use or disclose Protected Health Information other than as permitted by law or required by this Agreement;
b. Use appropriate safeguards to prevent the known or suspected use or disclosure of Protected Health Information other than as provided for by this Agreement, and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of any Electronic Protected Health Information that BUSINESS ASSOCIATE creates, receives, maintains, or transmits on behalf of COVERED ENTITY;
c. Limit any use, disclosure, or request for use or disclosure of PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with the requirements of HIPAA;
d. Comply, where applicable, with the applicable provisions of the Security Rule, including but not limited to matters involving electronic PHI;
e. Report any use or disclosure of information not provided for in this agreement, including breaches of unsecured PHI to COVERED ENTITY within thirty (30) days of BUSINESS ASSOCIATE becoming aware of such breach;
f. Mitigate, to the extent practicable, any harmful effect that is known or suspected to BUSINESS ASSOCIATE of a use or disclosure of Protected Health Information by BUSINESS ASSOCIATE in violation of the requirements of this Agreement;
g. Report to COVERED ENTITY any known or suspected Security Incident of which BUSINESS ASSOCIATE becomes aware, as well as any use or disclosure of Protected Health Information that is in violation of the requirements of this Agreement;
h. Ensure that any agents, including a subcontractor, to whom BUSINESS ASSOCIATE provides Protected Health Information agrees to the same restrictions and conditions that apply through this Agreement to BUSINESS ASSOCIATE with respect to such Protected Health Information;
i. If applicable, provide access, at the request of COVERED ENTITY, to Protected Health Information in a Designated Record Set, to COVERED ENTITY or, as directed by COVERED ENTITY, to an Individual in order to permit COVERED ENTITY to meet the requirements under 45 CFR 164.524;
j. If applicable, make any amendment(s) to Protected Health Information in a Designated Record Set that the COVERED ENTITY directs or agrees to pursuant to 45 CFR 164.526 at the request of COVERED ENTITY or an Individual, and at a time and in a manner prescribed by 45 CFR 164.526;
k. Document such disclosures of Protected Health Information 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 Protected Health Information in accordance with 45 CFR 164.528;
l. Provide to COVERED ENTITY or, as directed by COVERED ENTITY, to an Individual, information collected in accordance with Section 3(k) of this Agreement, to permit COVERED ENTITY to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528; and
m. Make BUSINESS ASSOCIATE'S internal practices, books and records relating to the use and disclosure of Protected Health Information available to the Secretary of Health and Human Services for purposes of determining the COVERED ENTITY'S compliance with HIPAA, ARRA and HITECH Regulations.

4. Business Associate Obligations for Security Safeguards

During the term of the Agreement, BUSINESS ASSOCIATE covenants and agrees that it, and any subcontractors with whom the BUSINESS ASSOCIATE contracts, shall comply with the terms and conditions associated with the provisions stated within the American Renewal and Revitalization Act, §13401, §13402 and §13404, §13405 and any other applicable areas including:

a. Implement and maintain reasonable protections for known and suspected data security threats and risks
b. Implement and maintain reasonable administrative, physical, and technical safeguards consistent with the COVERED ENTITY's that appropriately protect the confidentiality, integrity, and availability of the Protected Health Information that BUSINESS ASSOCIATE creates, stores, accesses, receives, maintains, or transmits on behalf of the COVERED ENTITY.
c. Designate an individual or individuals to serve as security officer(s) responsible for supervising the security and privacy mechanisms, including administrative, physical and electronic mechanisms, employed within the organization to prevent unauthorized access to PHI maintained on behalf of COVERED ENTITY.
d. At its own expense and at BUSINESS ASSOCIATE'S site, provide and maintain the equipment, software applications and testing services necessary to effectively secure and preserve the integrity and privacy of all PHI it maintains on behalf of COVERED ENTITY.
e. Maintain documented policies, procedures and documentation as may be necessary to prevent unauthorized parties from having access to, using, disclosing, processing, copying, modifying, corrupting, rendering unavailable, introducing computer code into or otherwise performing activities or operations upon or harmful to the availability, accessibility, integrity, privacy, structure, format or content of PHI maintained by the BUSINESS ASSOCIATE on behalf of COVERED ENTITY.
f. Maintain adequate processes, technologies, tools and procedures for identifying, reporting and mitigating, any deleterious effects from any system compromise or other improper use and/or disclosure of PHI maintained by the BUSINESS ASSOCIATE.
g. Notify COVERED ENTITY immediately in the event of any proven or suspected security incident in which there is reason to believe that any unauthorized person may have had access to the PHI stored on BUSINESS ASSOCIATE systems.
h. Conduct regular independent assessments of the policies, procedures, mechanisms and systems used by BUSINESS ASSOCIATE'S to fulfill the obligations of this Section, (i) no less frequently than once each year, and (ii) in response to any material breach of privacy or security within the scope of this Section.
i. Not electronically transmit PHI obtained by COVERED ENTITY over any open network unless such transmission is authorized by COVERED ENTITY, and only if such transmitted information is encrypted or secured from unauthorized access or modification in a manner that is consistent with 45 C.F.R. § 164.312(e)(1) of the Security Standards. For purposes of this section, the term "open network" includes the Internet, Extranets (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dialup lines, and private networks. For purposes of this section, the term "encryption" means the reversible coding or scrambling of information so that it can only be decoded and read by someone who has the correct decoding key. If Business Associate stores, uses or maintains PHI in encrypted form, or in any other secured form that is consistent with 45 C.F.R. § 164.312(e)(1) of the Security Standards, Business Associate shall promptly, at COVERED ENTITY request, provide COVERED ENTITY with the key or keys to decrypt such information and will otherwise assure that such PHI is accessible by COVERED ENTITY whenever reasonably requested.

j. In the event BUSINESS ASSOCIATE performs functions or activities involving the installation or maintenance of any software (as it functions alone or in combination with any hardware or other software) that is used to access, maintain or transmit PHI, BUSINESS ASSOCIATE shall ensure that all such software complies with all applicable standards and specifications required by the HIPAA Regulations and shall inform COVERED ENTITY of any software standards or specifications not compliant with the Security Standards.
k. Put into practice notification processes to comply with §13402 of the ARRA.
l. Obtain business associate agreements, which comply with the Privacy and Security Rules, with the parties with whom the BUSINESS ASSOCIATE contracts for services involving PHI.
m. In the event the BUSINESS ASSOCIATE becomes aware of noncompliance by its subcontractor(s), the BUSINESS ASSOCIATE is required to respond in the same manner as a covered entity that has become aware of noncompliance by its business associate.
n. Pursuant to 45 C.F.R. § 164.504(e)(2)(H) and (I), BUSINESS ASSOCIATE agrees to comply with requirements of the Privacy Rule that applied to COVERED ENTITY in the performance of such obligation.

5. Audits, Inspection, and Enforcement

Upon reasonable notice, COVERED ENTITY or their approved designee will independently inspect the facilities, systems, technologies, ~~books~~, and records of BUSINESS ASSOCIATE to monitor compliance with this agreement. The BUSINESS ASSOCIATE is expected to comply with any reasonable requests for systems access, data, or, information, in a timely manner in the format requested by the COVERED ENTITY or their approved designate. The fact that COVERED ENTITY or their approved designee inspects, or fails to inspect, or has the right to inspect, BUSINESS ASSOCIATE's facilities, systems, and procedures does not relieve BUSINESS ASSOCIATE of its responsibility to comply with this agreement, nor does COVERED ENTITY (i) failure to detect or (ii) detection, but failure to notify BUSINESS ASSOCIATE or require BUSINESS ASSOCIATE's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of COVERED ENTITY enforcement rights under the Agreement.

6. Term and Termination

a. The term of this Agreement shall be effective as of the date first set forth above and shall terminate when all of the Protected Health Information is destroyed or returned to COVERED ENTITY, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.
b. Upon COVERED ENTITY'S knowledge of a material breach of this Agreement by BUSINESS ASSOCIATE, COVERED ENTITY shall provide a reasonable opportunity for BUSINESS ASSOCIATE to cure the breach, and COVERED ENTITY may terminate this Agreement (and, if applicable, any agreement pursuant to which Services are provided) if BUSINESS ASSOCIATE does not cure the breach within a reasonable amount of time after notice is provided to the BUSINESS ASSOCIATE, or may immediately terminate this Agreement (and, if applicable, any agreement pursuant to which Services are provided) if BUSINESS ASSOCIATE has breached a material term of this Agreement and cure is not possible.

7. Effect of Termination

a. Except as provided in paragraph (b) of this Section, upon termination of this Agreement for any reason, BUSINESS ASSOCIATE shall return or destroy all Protected Health Information that it does not need to retain for record retention, audit or regulatory purposes. This provision shall also apply to Protected Health Information that is in the possession of subcontractors or agents of BUSINESS ASSOCIATE. BUSINESS ASSOCIATE shall only retain the least amount of PHI necessary for its own record retention, audit or regulatory purposes. This provision shall survive termination or expiration of this Agreement for any reason.

b. In the event that BUSINESS ASSOCIATE determines that returning or destroying Protected Health Information is infeasible, BUSINESS ASSOCIATE shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as BUSINESS ASSOCIATE maintains such Protected Health Information. This provision shall survive termination or expiration of this Agreement for any reason.

8. Re-Negotiation

The parties agree to negotiate in good faith any modification to this Agreement that may be necessary or required to ensure consistency with amendments to and changes in applicable federal and state laws and regulations, including but not limited to, the HIPAA, ARRA and HITECH Regulations.

9. Indemnification

BUSINESS ASSOCIATE shall indemnify, hold harmless, and defend COVERED ENTITY from and against any and all claims, demands, liabilities, judgments or causes of action of any nature for any relief, elements of recovery or damages recognized by law (including without limitation, attorney's fees, defense costs, and equitable relief), for any damage or loss incurred by COVERD ENTITY arising out of, resulting from, or attributable to any acts or omissions or other conduct of BUSINESS ASSOCIATE or its agents in connection with the performance of BUSINES ASSOCIATE'S or its agent's duties under this agreement. COVERED ENTITY shall indemnify, hold harmless, and defend BUSINESS ASSOCIATE from and against any and all claims, demands, liabilities, judgments or causes of action of any nature for any relief, elements of recovery or damages recognized by law (including without limitation, attorney's fees, defense costs, and equitable relief), for any damage or loss incurred by BUSINESS ASSOCIATE arising out of, resulting from, or attributable to any acts or omissions or other conduct of COVERED ENTITY or its agents in connection with the performance of COVERED ENTITY'S or its agent's duties under this agreement.

10. Miscellaneous Provisions

a. A reference in this Agreement to a section in the HIPAA, ARRA or HITECH Regulations means the section as in effect or as hereafter amended.
b. This Agreement constitutes the entire Agreement between COVERED ENTITY and BUSINESS ASSOCIATE regarding the subject matter hereof and supersedes all prior agreements (written or oral) relating thereto. Without limiting the generality of the foregoing, in the event of a conflict between the terms of this Agreement and any prior agreement (written or oral) pursuant to which BUSINESS ASSOCIATE is providing Services, the terms of the Agreement shall be controlling and such prior agreement shall be deemed to be amended hereby to the extent necessary to resolve such conflict. This Agreement shall be amended or modified only by a writing signed by COVERED ENTITY and BUSINESS ASSOCIATE.
c. Any ambiguity in this Agreement shall be resolved in favor of a meaning that requires or permits COVERED ENTITY to comply with the HIPAA, ARAA or HITECH Regulations.

d. This Agreement shall be governed by and construed in all respects accordance with the substantive and procedural laws of the State of New York applicable to agreements made and to be performed entirely within such State, without regard to principles of conflicts of laws or statutes, except solely to the extent that HIPAA and/or the HITECH Act preempt the laws of New York, in which event HIPAA and/or HITECH Act shall govern this agreement as applicable.

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

The Arc of Monroe

By: _____ By: _____

(Signature) (Signature)

Name: _____ Print Name: _____

Title: CFO

Date: _____ Date: _____

v. 10.20