Topic: Disclosures of Protected Health Information (PHI) for Treatment, Payment and Health Care Operations (TPO); Data Use Agreements and Limited Data Sets	**Department:** Entire Agency
Original effective date: 4/1/03	**Last revision date:** 11/15/24
Owner: VP for Quality and Compliance	**Frequency of reviews:** Annual
Internal/Regulatory Reference(s) (all that apply): 164.506(a); NYS PHL §17	
Related documents/Links:	

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

Additional Information: "Treatment" is defined as the provision, coordination, or management of health care and related services. Under HIPAA, the work we do with the people we support is considered "health care." This includes the coordination or management of health care by The Arc with an outside provider (such as an outside doctor). It also includes the referral of a patient for health care from one health care provider to another (such as from The Arc to another provider). In addition, per NYS Public Health Law (PHL) §17, upon written request of a competent person we support or a guardian appointed under MHL §81, we are required to release and deliver all medical records regarding the person we support to any other designated physician or hospital.

EXAMPLES: Implementing a staff action plan, taking data, giving someone medications, implementing a behavior support plan, using someone's IPOP to keep them safe, referring someone to another provider.

"Payment" is defined as activities undertaken by The Arc to obtain or provide reimbursement for the provision of health care. Specifically, this includes but is not limited to determining eligibility for coverage, and billing and claims management.

EXAMPLES: Using someone's name and Medicaid number to get paid for the services we provided them, submitting claims to Medicaid or Medicare, looking at someone's DDP score as it relates to acuity and rates.

"Health care operations" are defined activities which help the agency to run smoothly and compliantly. This includes but is not limited to the following:

- Quality assessment and improvement activities
- Activities related to Corporate Compliance
- Training
- Arranging for external audits, such as our annual financial audit
- Arranging for legal counsel
- Cost-management
- Strategic planning
- Business management
- Governance

EXAMPLES: conducting compliance or quality audits, providing training to staff, talking to our lawyers about a case, planning for how to move the agency forward to provide the best supports, Board committees, and the Board of Directors and its work.

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. In many cases, before staff can use or share PHI, we need to have a signed authorization from the person or their legal representative, giving us permission to do so. Please cross reference the policy, "Authorizations for Use and Disclosure."	Staff
2. There are 3 primary instances where we can use and/or share PHI without first getting authorization: *Treatment *Payment *Health care operations (often just called "operations") Please see definitions of these terms above. Minimum Necessary always applies. This means that staff can only use or share the least amount of information needed to do their work. Please cross reference the policy, "Staff Confidentiality of PHI and Minimum Necessary" for more information.	Staff
3. If staff have questions about whether something falls under Treatment, Payment or Operations, they should consult with their manager or the VP for Quality and Compliance	Staff

4. Similarly, staff should talk with their manager or the VP for Quality and Compliance if they have questions about whether an authorization is needed before PHI can be used or shared.	Staff
Deceased Individuals and Use/Disclosure of PHI:	
1. HIPAA rules apply to PHI about someone we support for a period of 50 years following their death.	Staff; Management; VP for Quality and Compliance
De-identified Information	
1. De-identified information means that if you read it, you can't tell who it's about. The process to make PHI de-identified is spelled out clearly in the regulations. Specifically, to make PHI de-identified, all of the following has to be removed: *Names or initials *All location names smaller than a state. This includes street address, city, county, precinct and zip code *Data information for dates directly related to the person, except the year. The year can be included unless the person is over 89 years old. This includes birth date, admission date, discharge date, and date of death. *Telephone numbers *Fax numbers *Email addresses *Social security numbers *Medical record numbers *Health insurance numbers *Account numbers *Certificate/license numbers *VIN and license plate numbers *Device identifiers and serial numbers *URLs that relate to the person *IP Address numbers that relate to the person *Biometrics such as finger or voice prints *Full face photos or other photos that identify the person (see definition above) *Any other unique identifying number, characteristic or code that can be used to identify them Only a manager or the VP for Quality and Compliance or their designee are authorized to de-identify PHI.	Manager or the VP for Quality and Compliance
2. Staff are required to consult with a manager and/or the VP for Quality and Compliance before initiating the de-identification of PHI or if they have PHI that they feel needs to be de-identified.	Staff
Limited Data Set Usage and Data Use Agreements (DUAs)	
1. The Arc may use or disclose a limited data set if we enter into a "data use agreement" (DUA) with whomever we wish to send the limited data set to.	Managers, VP for Quality and Compliance

2. Under the "data use agreement," the recipient of the data must: *Identify who is permitted to use or receive the limited data set *Not use or further disclose the limited data set except as permitted by the DUA *Use appropriate safeguards to prevent the use or disclosure of the PHI outside the terms of the DUA *Report to The Arc if it learns that the limited data set was used or disclosed outside the terms of the DUA *Ensure that anyone that it provides the limited data set to also agree to the same restrictions and conditions of the DUA *Not identify the information or contact the people whose information it is	VP for Quality and Compliance
3. A limited data set is PHI that excludes the following direct identifiers of the person, or of relatives, employers, or household members of the person: *Names or initials *Postal address information, other than town or city, state, and zip code *Telephone numbers *Fax numbers *Email addresses *Social security numbers *Medical record numbers *Health plan beneficiary numbers *Account numbers *Certificate/license numbers *Vehicle identifiers and serial numbers, including license plate numbers *Device identifier and serial numbers *Web URLs *IP Address numbers *Biometric identifiers, including finger and voice prints; AND *Full face photographic images and any comparable images	Managers, VP for Quality and Compliance
Manager responsibilities:	
1. Managers are responsible for acting as role models for other staff in regards to keeping PHI as secure as possible.	Managers
2. Managers should have a solid understanding of what actions constitute treatment, payment or healthcare operations, as defined in this policy.	Managers
3. Managers should have a basic understanding of when an authorization is required before PHI can be used or disclosed; or know from whom they can seek support in making that determination.	Managers
4. Managers should have a basic understanding of what the de-identification of PHI entails. They should reach out to the VP for Quality and Compliance for guidance and support to ensure that they are meeting the requirements.	Managers
5. Managers may be asked to assist with pulling together a limited data set, per this policy.	Managers
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. Responsible for conducting or providing guidance and direction regarding de-identification of PHI when requested within the requirements of the HIPAA rule.	VP for Quality and Compliance
4. Acts as a resource for staff in regards to proper implementation of the HIPAA privacy rule	VP for Quality and Compliance
5. Has primary responsibility for compiling a limited data set and administering a Data Use Agreement	VP for Quality and Compliance

Document revision record:

Revision Date	**Release Date**	**Reason for change**	**Approver**
9/12/08	9/12/08	Reasons for change not documented	P Dancer
10/21/11	10/21/11	Reasons for change not documented	P Dancer
7/25/17	7/25/17	Reasons for change not documented	P Dancer
11/20/18	11/20/18	Reasons for change not documented	P Dancer
1/25/21	1/25/21	Transitioned to new procedural format and clarified some aspects	P Dancer
11/15/21	11/15/21	Corrected typo	ICC
12/8/21	12/15/21	Added reference to PHL §17.	ICC
12/20/23	12/20/23	Added cross-referenced policies; added "designee" to the VPQC where appropriate; added that staff should consult with management if they have PHI to de-identify; managers' understanding of what de-identification entails and who can do it	ICC
11/25/24	11/25/24	Added clarifying language and removed inconsistent language; strengthened directives regarding de-identification	ICC