Topic: Staff confidentiality of Protected Health Information (PHI) and Minimum Necessary	**Department:** Entire Agency
Original effective date: 4/1/03	**Last revision date:** 10/23/24
Owner: VP for Quality and Compliance	**Frequency of reviews:** Annual
Internal/Regulatory Reference(s) (all that apply): 164.502	
Related documents/Links: Media Protection v1 3.2022.pdf	

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: The Arc of Monroe is a covered entity as defined in the HIPAA Rule and, as such, is committed to keeping the health information about the people we support private and to follow the requirements of The Rule.

"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.

"Minimum necessary" means that people can only use or share the least amount of PHI that they need to doaccomplish the task at hand. Example: if a staff person only needs to know about a person's recent hospital stay, they can't hear about something that happened to the person as a child or other services and supports.

Medicaid Confidential Data (MCD) is defined as any information or data received directly or indirectly from the New York State Department of Health (NYSDOH) about individuals who have applied for or received Medicaid benefits, including Medicaid claims data, names and addresses, diagnoses, medical services, and other personally-identifiable information. We are only likely to receive MCD indirectly from another provider or organization with whom we have a contractual arrangement and not directly from the NYSDOH.

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

Procedure	
Task:	**Responsible party:**
General Guidelines	
1. Staff may routinely use PHI about people we support in order to carry out their duties. This may mean using it within the agency or sharing it with others outside the agency who also serve the person supported. This applies to use or disclosure of PHI in any form or format, including verbal/ASL, handwritten or electronic.	Staff
2. In all aspects of their work, staff must take steps to ensure that PHI is kept confidential. Reminders: *Staff should be careful about sharing PHI verbally or using ASL, keeping in mind that others may be within earshot or visual range *If staff see PHI in a form or location where people with no right to it may see or access it, they are obligated to take steps to ensure its privacy Failure to take appropriate steps to ensure the confidentiality of PHI can result in disciplinary actions up to and including termination of employment.	Staff
3. Anytime staff see, use or share PHI, it can only be the least amount of information needed to do one's job or carry out a specific task. This is a requirement of HIPAA law and is referred to as "Minimum Necessary."	Staff
4. These standards apply to both routine (happen frequently) and non-routine (don't happen very often) situations.	Staff
5. If staff has questions about HIPAA including how to apply the minimum necessary standard, they can consult with their manager or the VP for Quality and Compliance	Staff
6. Failure to follow the minimum necessary standard may be considered a violation of HIPAA and could result in disciplinary actions up to and including termination	Managers
7. To the extent the agency receives and/or maintains Medicaid Confidential Data (MCD), it will comply with all related contractual requirements	Staff/Managers
PHI, cameras, semi-public spaces and social media	
1. Staff can only take pictures of people we support on an Arc cell phone, tablet or digital camera with a valid HIPAA-compliant photo release/authorization in place. They may not take them on personal cell phones.	Staff
2. Staff should never post PHI where people may randomly see it, such as people passing by their workspace or office.	Staff
3. Artwork created by people we support that identifies them as a service recipient (i.e., is attributed to them and states that they attend a certain program) can be hung or shared anywhere if we have a signed authorization from them or their legal representative which says we can. If we don't have a signed authorization, such artwork cannot be hung in	Person we support/legal representative Management

entryways, lobbies or any area of the site where the public can come into; nor can it be shared outside the agency. It would be OK for it to be hung elsewhere in the facility (places where members of the public would need permission to enter, such as hallways past the receptionist, core rooms, living rooms, bedrooms, etc.). It is management's responsibility to ensure this it followed. If the artwork does not identify the artist as a service recipient, the artwork can be hung anywhere without restriction or need for an authorization.	
4. Staff are NOT allowed to post any PHI directly to any personal social media site or platform (including but not limited to Facebook, Twitter/X, Instagram, Pinterest, Snapchat, WeChat, TikTok, Tumblr, YouTube, etc.). This applies: *Whether the person whose information is to be shared says it's OK for staff to do it *Whether the person whose information is to be shared has signed an agency authorization *Whether others have already done it Only staff authorized by The Arc can share or post pictures of people we support on social media on behalf of The Arc. This is typically done through our Marketing and Communications department. Staff can ONLY repost or "like" posts containing PHI (including pictures) made by The Arc on its official sites or information that the person themself has posted (we cannot do the original posting for them; they need to do that on their own or with the help of someone other than staff). Failure to comply could result in disciplinary actions up to and including termination of employment.	Staff
Databases and workstations:	
1. Staff must lock or sign off from their computer when they are away from it.	Staff
2. Staff must log out of computer systems that have PHI on them when they are done using them. This includes but is not limited to our electronic health record, eVero, Millin, etc.	Staff
3. Staff is responsible for their login names and passwords. Passwords should NEVER be stored with the device they apply to. EXAMPLE: you should NEVER store your laptop encryption password with the laptop itself. This includes taping it to the laptop or "hiding it" by storing it in the battery compartment. Passwords should never be left on or near your primary work station. You are responsible for anything that happens within an electronic system under your user name and password. The Arc reserves the right to monitor who accesses which business-related computer systems and for what purposes.	Staff, IT/CIS

Downloading, copying or removing PHI:	
1. Staff are not allowed to download, copy or take any PHI from the agency for personal reasons. Doing so could result in disciplinary actions up to and including termination of employment. Any information downloaded, copied or taken for business reasons must be returned before the person leaves the agency or has a change in their role. This includes PHI on their personal cell phone, if they were given permission to use it for work.	Staff
2. Please cross reference the policy, "Media Protection" for further information (see header for link)	Staff
Emailing, texting, faxing, and mailing PHI:	
1. Staff needs to encrypt any email that: *Has PHI in it AND *Is being sent outside the agency – meaning, to any email address that ends in something other than "@arcmonroe.org." To encrypt email, staff just needs to type the word "secure" somewhere in the subject line (staff do not need to encrypt emails sent to email addresses ending in "@arcmonroe.org"). Failure to encrypt when necessary could result in disciplinary action up to and including termination. Texting of PHI is not allowed on any device, including agency-issued devices without express permission from a member of the Executive Management Team (CEO, COO, CHRO, CFO) or the VP for Quality and Compliance. PHI is not adequately protected from being compromised via texting.	Staff
2. If someone we support or their legal representative wants staff to send unencrypted emails to them, please refer to the policy on "PHI and email" for the details on how to do this within HIPAA requirements.	Staff
3. While faxes are relatively safe, please verify the fax number before sending and be sure to include a cover sheet that references confidentiality. If you ever discover you sent a fax to the wrong number, please notify the recipient that they received a fax in error and let your manager know immediately. The manager will notify the VP for Quality and Compliance	Staff Manager
4. Before mailing any correspondence that contains PHI: *Please confirm that you are sending the right information to the right place *Please be sure that the address you are sending to is correct (house number, apartment number, street name, city and zip code). This includes email. Please verify that all of the emails on the distribution list are accurate and ensure that autofill has not inserted the incorrect address. *Be very careful about "replying all," as there may be people on the email distribution list that should not be included on your response.	Staff

Manager responsibilities:	
1. Managers have an enhanced responsibility in regards to HIPAA. Specifically: *They have an obligation to act as a role model for other staff in using and disclosing PHI appropriately; establishing a culture of sensitivity around PHI; teaching staff about the importance of treating PHI confidentially; and responding if/when issues are identified. *They are responsible for having a basic understanding of HIPAA requirements – including what constitutes "minimum necessary" – and for knowing where to obtain additional information if needed. *If they see a situation which puts any PHI at risk for improper disclosure, they have an obligation to respond immediately to mitigate the risk. Example: if they see unsecured PHI in a public or semi-public place where others could access it (such as in a trash bin outside a facility), they must respond immediately to ensure the PHI is secure. Failure to take steps to secure PHI as appropriate can result in disciplinary actions up to and including termination of employment.	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. Acts as a resource for staff in regards to proper implementation of the HIPAA privacy rule	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
7/29/15	7/29/15	Reasons for change not documented	P Dancer
9/29/16	9/29/16	Reasons for change not documented	P Dancer
7/25/17	7/25/17	Reasons for change not documented	P Dancer
11/19/18	11/19/18	Reasons for change not documented	P Dancer
1/25/21	1/25/21	Transitioned to new procedural format and clarified some aspects	P Dancer
9/29/21	10/8/21	Clarified that artwork unattributed to a person we support can be hung anywhere; clarified that PHI must be returned upon change of role as well as leaving the agency	ICC
10/5/22	10/13/22	Consolidated the former "minimum necessary" policy into this policy; cross-referenced the "Media Protection" policy; added language regarding MCD	ICC
10/30/23	10/30/23	Added language about texting PHI to the procedure	ICC

9/26/24	10/23/24	Added clarifying language, modified guidance on taking pictures on cell phones, added a caution on replying all to emails received	ICC