

Topic: Staff confidentiality of Protected Health Information (PHI) and Minimum Necessary	Department: Entire Agency
Original effective date: 4/1/03	Last revision date: 8/21/26
Owner: VP for Quality and Compliance (VPQC)	Frequency of reviews: Annual
Internal/Regulatory Reference(s) (all that apply): 45 CFR § 164.502; 45 CFR § 164.514(d); 45 CFR § 164.530(a); 45 CFR § 164.530(c); 45 CFR § 164.508	
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: The Arc is a covered entity as defined in the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and, as such, is committed to keeping the health information about the people we support private and following the requirements of the Privacy Rule. The VPQC acts as the agency’s Privacy Officer and administers HIPAA privacy policies and procedures.

“Protected health information (PHI)” is information about people we support that relates to their past, present, or future physical or mental health or condition, the health care provided to them, or payment for that health care, and that identifies them or could reasonably be used to identify them. In addition to more obvious examples such as treatment plans, service documentation, clinical assessments, the following should also be 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, or another distinctive physical characteristic.
- 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” generally means making reasonable efforts to use, disclose, or request only the amount of PHI reasonably necessary to accomplish the intended purpose. HIPAA identifies certain situations in which the minimum necessary standard does not apply, including certain disclosures for treatment and disclosures to the person who is the subject of the information or their personal representative. Example: If a staff person only needs information about a person’s recent hospital stay to perform a particular task, they should not access or receive unrelated information about the person’s history 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.

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

Procedure	
Task:	Responsible party:
General Guidelines	
1. Staff may use or disclose PHI as necessary to carry out their assigned duties and as permitted by HIPAA, other applicable law, and Arc policy. This may include sharing PHI with external providers or other authorized parties involved in the person’s services when the disclosure is permitted.	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 may result in disciplinary action up to and including termination of employment.	Staff
3. When the HIPAA minimum necessary standard applies, staff must make reasonable efforts to use, disclose, or request only the PHI reasonably necessary to accomplish the intended purpose.	Staff
4. If staff have questions about HIPAA, including how to apply the minimum necessary standard, they should consult their manager or the Privacy Officer.	Staff
5. To the extent The Arc receives or maintains Medicaid Confidential Data (MCD), it will comply with all related contractual requirements. Staff who access or handle MCD must comply with applicable contractual requirements and Arc procedures governing that information.	Staff; Management
6. Managers who become aware of PHI that is unsecured or at risk of improper use or disclosure must take immediate reasonable steps to secure the information, mitigate further disclosure, and ensure the matter is reported to the Privacy Officer.	Management
PHI, cameras, semi-public spaces and social media	
1. Staff may take pictures of people we support only on an Arc-issued cell phone or tablet with the required software installed, and only when a valid HIPAA-compliant photo release/authorization is in place for the person supported. Pictures may not be taken on personal cell phones. Staff should consult The Arc’s IT Department for information about obtaining the required application.	Staff
2. Staff should never post PHI where people may randomly see it, such as people passing by their workspace or office.	Staff

3. As an Arc workforce requirement, staff may not post PHI about people we support to personal social media accounts or platforms, including social networking, photo/video sharing, messaging, and similar services, even when the individual has consented or signed an authorization permitting The Arc to use or disclose the information. 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 platforms, or information that the person themselves 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
Artwork:	
1. 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) may be displayed or shared if a signed authorization from the person or their personal representative permits it.	Staff
2. Without a signed authorization, such artwork may not be displayed in entryways, lobbies, or other areas of the site that the public may enter, and may not be shared outside The Arc. The artwork may be displayed elsewhere in the facility where members of the public would need permission to enter, such as hallways beyond the reception area, core rooms, living rooms, or bedrooms. Management is responsible for ensuring compliance with this requirement.	Staff; Management
3. If the artwork does not identify the artist as a service recipient, it may be displayed anywhere without restriction and without an authorization.	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, and Millin.	Staff
3. Passwords and other authentication credentials must be stored and managed only in accordance with Arc information-security requirements and must not be stored with the device to which they apply. For example, a laptop encryption password must not be taped to or stored with the laptop. Staff are responsible for protecting their credentials and must not permit others to use their accounts.	Staff, IT/CIS

The Arc reserves the right to monitor who accesses which business-related computer systems and for what purposes.	
Downloading, copying or removing PHI:	
1. Staff may not download, copy, remove, or retain PHI for personal purposes. Staff may be authorized to use personal devices for limited agency-related purposes, such as accessing Arc email or other approved systems. PHI and other agency information may not be downloaded or stored locally on a personal device unless specifically authorized by The Arc. When a staff member leaves The Arc, changes roles, or no longer requires such access, all Arc-related information and access must be removed from the personal device as directed by The Arc.	Staff
2. Please cross reference the HIPAA Security policy, "Media Protection" for further information.	Staff
Emailing, texting, faxing, and mailing PHI:	
1. Staff must encrypt any email containing PHI that is sent outside The Arc. To encrypt the email and any attachments, type the word "secure" anywhere in the subject line. Failure to encrypt when necessary could result in disciplinary action up to and including termination. Because ordinary text messaging is not an Arc-approved method for transmitting PHI, staff may not text PHI on personal or agency-issued devices unless expressly authorized by a member of the Executive Management Team or the Privacy Officer. Exceptions may be made when necessary to address an emergency or other urgent situation, consistent with agency direction.	Staff
2. 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
3. If a person we support or their personal representative requests that PHI be sent to them by unencrypted email, staff should follow the requirements in the PHI and Email policy.	Staff
4. Before faxing PHI, staff must verify the fax number and use the required confidentiality cover sheet. If staff discover that PHI was faxed to the wrong recipient, they must immediately inform their manager. The manager must promptly notify the Privacy Officer. Reasonable efforts should be made to contact the unintended recipient and request that the information be returned or securely destroyed.	Staff; Management
5. Before mailing any correspondence that contains PHI: - Confirm that you are sending the correct information to the correct recipient. - Verify that the mailing address is correct, including house number, apartment number, street name, city, and ZIP code.	Staff

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 procedure format/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 Arc	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
9/22/25	10/23/25	Added clarifying language; removed an obsolete reference	ICC
8/21/26	8/21/26	Added clarifying language; removed discrete manager and VPQC sections, streamlined language and removed redundancies	ICC