Topic: PHI and Email	**Department:** Entire Agency
Original effective date: 6/1/03	**Last revision date:** 1/26/21
Owner: VP for Quality and Compliance	**Frequency of reviews:** Annual
Internal/Regulatory Reference(s) (all that apply): 164.312(e)(2)(ii)	
Related documents/Links:	

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, "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. Before sending an email, staff should review the distribution list carefully to ensure they have the correct addresses listed before hitting "Send." If staff type only part of a recipient's name, Microsoft Outlook often autofills the incorrect name, so this is a critical step. PHI sent to an incorrect recipient, even if done accidentally, would still be a HIPAA violation.	Staff

2. Whenever sending PHI to an email outside The Arc of Monroe, the email needs to be encrypted by typing the word Secure somewhere in the subject line. "Outside the Arc of Monroe" means to an email address ending in anything other than "@arcmonroe.org." Note: Emails with PHI sent to another Arcmonroe.org email address are automatically secured because they are within the same system. Staff do not need to include the word Secure in the subject line of internal emails containing PHI.	Staff
3. As with any use or disclosure of PHI, staff can only include the least amount of information needed to complete the task at hand.	Staff
4. Staff should be especially careful with "reply all" when responding to emails. They should ensure that everyone on the distribution list needs to get their reply.	Staff
5. If someone we support or their legal representative would prefer to receive unsecured emails from us – including emails containing PHI, they need to tell us that that is what they would like. They should make this request in writing.	People we support or legal representatives
6. Once they do so, we need to tell them <u>in writing</u> that there is some risk: specifically, that by sending an unsecured email, someone could intercept the email and get access to the PHI. If they want us to send unsecured emails containing PHI, if someone intercepts the email containing PHI, they can't hold us responsible. Once we have told them this in writing, we can begin sending PHI via unsecured emails. This will remain in effect until the person or their legal representative requests formally (in writing) that we stop.	Manager
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 the provisions of this policy.	Managers
3. Managers should periodically reinforce with their teams the importance of securing email appropriately and being careful with autofill.	Managers
4. Managers should know where and from whom to obtain support should they have questions in enforcing 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. 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
9/17/07	9/17/07	Reasons for change not documented	P Dancer
9/17/08	9/17/08	Reasons for change not documented	P Dancer
10/24/11	10/24/11	Reasons for change not documented	P Dancer
11/16/12	11/16/12	Reasons for change not documented	P Dancer
9/30/16	9/30/16	Reasons for change not documented	P Dancer
12/28/18	12/28/18	Reasons for change not documented	P Dancer
1/26/21	1/26/21	Transitioned to the new procedural format	P Dancer
2/8/24	3/18/24	Reworded and relocated bullet on risks with Autofill; added that requests for unsecured emails should be in writing; added that such requests are in place until the person requests they stop	ICC