AGENCY POLICY:
STAFF CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION

SCOPE OF POLICY

This policy applies to all employees, trainees, volunteers, consultants, students, contractors and subcontractors at the agency. Everyone listed is required to follow this policy.

STATEMENT OF POLICY

The Arc wants to make sure that we keep health information about the people we support private. You can't share information about people we support with people who don't have the right to get it.

IMPLEMENTATION OF POLICY

A. Definition of Protected Health Information:

"Protected health information" means information about someone we support that:

- Identifies who they are AND
- Has something to do with their health.

"Identifies" them could mean a name, a description or a picture of them.

"Their health" could mean talking about a condition or disease they used to have, have now or could have in the future. It can be either mental or physical.

Examples:

- Someone used to have depression
- Someone has cerebral palsy
- Someone could develop diabetes

Protected health information can be written or spoken. Written includes on a computer.

Protected health information is also called PHI.

B. Public viewing/hearing:

Staff need to make sure PHI can't be seen or heard by others. Staff should be careful talking about PHI. They should do this in private locations so they can't be overheard.

Staff shouldn't post PHI where others can see. This would be things like a person's diagnosis or the things we need to do to help them.

Artwork and pictures of people we support doing things they like are a little different. They can't be posted in places where the public might see them unless we have permission. Example: artwork by a person we support cannot be hung in a day program lobby unless we have permission. Permission would come from them or their legal representative. Artwork could be hung elsewhere in the day program or in the person's home. If you're not sure, ask your manager. PHI should never be shared with the media without permission from management.

Social media can be hard to use and still follow HIPAA law. Here are some general rules:

- Staff cannot post PHI – including pictures of people we support – directly to or on their personal social media. This includes Facebook, Twitter, Instagram, Snapchat, Tumblr, etc.
    - It doesn't matter if the agency has an authorization or not – you still cannot do this
    - It doesn't matter if the person tells you it's OK – you still cannot do this
    - This includes backs of heads, side shots, direct full-face shots, close-up shots or those from a distance
- Initials are considered PHI. Reducing names to initials does not make it OK to share.
- Describing someone in a way that people will know who you're talking about makes that information PHI as well. HIPAA law actually lists out what you have to do so that something is no longer PHI. Please contact the VP for Quality and Compliance for details.
- If the person we support him/herself posts information about themselves, you can like and/or repost that information. You may not add additional information to the post that would be considered PHI. We cannot do the original posting for them. They have to post it on their own.
- If one person we support takes pictures of others we support and posts them, you can like and/or repost that information. You may not add additional information to the post that would be considered PHI. We cannot do the original posting for them. They have to post it on their own.
- If The Arc posts information about a person we support, you can like and/or repost that information. You may not add additional information to the post that would be considered PHI.
- In the interest of a consistent Arc social media approach, programs cannot create social media accounts for their individual programs and post PHI. All Arc-labeled social media posts need to come through Marketing.
- You cannot use any cell phone – including an agency-issued cell phone – to take pictures of PHI. This is because the cloud where data is stored is not considered secure. If/as this changes, we will keep you informed.
- If you wish to take pictures of people we support, please consider purchasing a digital camera. Once taken, pictures can be downloaded to an Arc computer and emailed directly to Marketing using your Arc account.

C. <u>Databases and Workstations:</u>
Staff need to log out of computer systems that have PHI in them when they are done using them. Especially when they leave their workstation. Examples: PrecisionCare and FundEZ. Doing that, others can't see things they shouldn't.

Staff is responsible for their login names and passwords. Passwords should not be put where others can see them. You cannot share them with other people. If you do and someone else does something wrong under your name, you will be responsible for what they did. The Arc monitors who gets into which computer systems and what they do in there.

Confidentiality of phi pnp

D. Downloading, Copying or Removing:
Staff cannot download, copy or take any PHI from the agency for personal reasons. They can only do this if they need it to do their job. If they leave the agency, they need to give this information back or prove that they destroyed it.

E. Emailing, Faxing and Mailing Information:
Staff need to encrypt any email that:

- Has PHI in it AND
- Is being sent outside the agency. This means to an email that does not end in "@arcmonroe.org".

To encrypt any email, staff need to type the work "secure" in the subject line of the email. It doesn't matter where the word is put in the subject line. If staff don't do this, they could receive discipline. Sometimes people in other companies who get encrypted email don't like it. They may ask you to send it without encryption. If it has PHI in it, you can't. If they refuse to accept encrypted email, talk to your supervisor.

If someone we support or their legal rep asks you to send them unencrypted emails or texts that have PHI, you have to do what they ask. Before you do, you need to tell them that there is some risk doing so and that they accept the risk. You can do this in an email. See policy on email for more detail.

Faxes are usually pretty safe. This is because they can't get intercepted while they're being sent. Staff needs to make sure they dial the correct number. They also need to include a cover sheet that talks about confidentiality. If you ever send a fax to the wrong place, please let your manager know right away.

Before you mail PHI somewhere, please:

- Double check the information you're sending. You want to make sure you're sending the right things.
- Double check the address where you are sending it.

Effective date: 4/1/03

Revised:
9/12/08
10/21/11
7/29/15
9/29/16
7/25/17
11/19/18