Topic: Breaches of PHI	**Department:** Entire Agency
Original effective date: 9/23/09	**Last revision date:** 1/25/24
Owner: VP for Quality and Compliance	**Frequency of reviews:** Annual
Internal/Regulatory Reference(s) (all that apply): 164.400-164.414	
Related documents/Links: HIPAA HITECH Breach Notification Risk Assessment Form	

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, "breach" is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA law which compromises the security or privacy of the PHI.

A breach does not include:

- When an Arc staff accidentally accesses PHI for one person when they were trying to look up someone else. For example, a staff person goes into our Electronic Health Record to look up John Smith but accidentally opens the record for Joan Smith.
- When an Arc staff unintentionally sends PHI to another Arc staff but shouldn't have. For example, a staff person thought that Sue Jones (Arc Staff) worked with someone we support. They send PHI about that person to Sue, but she doesn't really work with them (so doesn't have a right to that information).
- When PHI is shared in front of someone who would not be able to understand or retain the information. For example, a staff person shares PHI with another staff in front of someone who is sound asleep. Since they are asleep, they could not remember what was said.

"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. Information about employees is not considered PHI, as we are not a health-care provider to our employees.

"Unsecured PHI" means PHI that is not made unreadable or unusable through encryption or cross-cut shredding. Please note that documents shredded using "strip cut shredders" are still considered unsecured, as documents may be reassembled after shredding. Similarly, ripping up or using scissors to cut up PHI does not render it secured.

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

Procedure	
Task:	**Responsible party:**
General Guidelines	
1. Staff have a responsibility to keep all PHI secure and protected at all times. If they observe PHI at risk of improper access or breach, they have an obligation to respond immediately to secure the PHI. Failure to do so may result in disciplinary actions up to and including termination.	Staff
2. If staff believe that an improper disclosure or breach of PHI has occurred, they are to take steps to secure the PHI (if possible) and then notify their manager immediately.	Staff
3. Managers will assess the situation. If they believe that an improper disclosure or breach may have occurred (as defined in this policy), they will notify the VP for Quality and Compliance.	Managers
4. The VP for Quality and Compliance will confirm the following information with the manager: *Why the manager believes that an improper disclosure or breach occurred *What information was involved, including: names of people impacted and specific PHI involved in the breach *When the situation is believed to have occurred *When the situation was discovered *Who it is believed was involved in the improper disclosure or breach *What actions have been taken so far to secure the PHI (if possible) and address the concern	VP for Quality and Compliance
5. If it's determined that the situation may meet the criteria for a breach, the VP for Quality and Compliance will initiate a review or formal investigation (depending on the circumstances and complexity of the situation) to determine how it occurred, confirm if there was a breach as defined in the law, and what information was involved.	VP for Quality and Compliance; Investigator
6. The VP for Quality and Compliance will open a formal compliance case for the situation and notify members of EMT of the situation. Please cross reference the policy, "Management of Situations Reported to the Compliance Office." ****LINK****	VP for Quality and Compliance
7. Once the case has been resolved (investigations, notifications to people supported, and the program has responded), the compliance case will be presented to and reviewed by the Internal Compliance Committee.	VP for Quality and Compliance
8. Business Associates are required to inform us if they think they have a breach involving any of our PHI. Please cross reference the policy on Business Associates for more information.	Business Associates
9. Documentation regarding confirmed HIPAA breaches will be kept for at least 6 years from the date of the breach.	VP for Quality and Compliance

Risk assessment:	
1. Based on the review or investigation, the VP for Quality and Compliance will conduct a risk assessment to determine if a breach actually occurred, as defined in the law. This assessment is designed to determine whether the PHI was considered "compromised" (using the language of the law). A number of factors may lead to a determination that it was not, including but not limited to: *Was the PHI sent to another organization (or their staff) who are bound by HIPAA law (so they understand the need to keep PHI secure) *Were we notified of the breach immediately when it was received by the person who shouldn't have gotten it *Did the recipient confirm that the information was not disclosed beyond them *Did the recipient confirm that the PHI has been shredded or is being mailed back *The specific PHI was not considered overly sensitive to the point where it could be used to the detriment of the person (I.e., was it only a document with initials on it or did it include things like social security number, health insurance information, DOB, full name and address, etc.). *Level of risk based on the type of PHI involved in the disclosure	VP for Quality and Compliance
2. The risk assessment will be documented on a standard form (see attached) and added to the compliance case file.	
For confirmed breaches involving <u>fewer than 500 people</u> we support:	
1. If it was confirmed through the risk assessment that the situation met the criteria for a breach AND the breach involved <u>fewer than 500</u> people, the people affected by the breach need to be informed in writing. This needs to occur within 60 days of when we first discovered the breach. This notification should come from the director or senior director of the program. The VP for Quality and Compliance will provide necessary support in the development of this letter.	Managers, VP for Quality and Compliance
2. This notification letter must be written in simple language and include the following information: *What happened and when *What PHI was breached *Things that the person can/should do in response to the breach (i.e., monitor their credit) *What we're doing to find out how it happened *What we're doing to prevent it from happening again *What we're doing so that people aren't hurt by the breach *Who they can call with questions.	Managers
3. This letter needs to be hard-copy mailed to the last known address of the person whose information was breached unless the person prefers to receive this via email. If the person whose information was breached is deceased, we need to send the letter to the last known address of their next of kin.	Managers
4. If our contact information is out of date for fewer than 10 people, we can let them know in other ways, such as by phone. Any alternate communications must be documented in our Electronic Health Record	Managers

5. If our contact information is out of date for more than 10 people, we are required to: *Put something about the breach on our webpage; OR *Put something out in the local media. Both of these must include a toll-free number where people can call to find out if they were affected by the breach. The VP for Quality and Compliance will assist managers in this situation.	Managers, VP for Quality and Compliance
6. Managers are also required to respond to the findings of the review or investigation and provide the following information: *Actions being taken to prevent recurrence of the breach *Information on any disciplinary actions take with staff	Managers
7. Managers should keep a copy of the letters for their records, but also send a copy to the VP for Quality and Compliance to include with the compliance case record, and for the FTC notification which will need to occur.	Managers
8. Within the first 60 days of the calendar year following the breach, the FTC will be notified of the breach consistent with the procedures.	VP for Quality and Compliance
For confirmed breaches involving <u>more the 500 people</u> we support:	
1. If it was confirmed through the risk assessment that the situation met the criteria for a breach AND the breach involved <u>more than 500 people</u>, the people affected by the breach need to be informed in writing. This needs to occur within 60 days of when we first discovered the breach. This notification should come from the director or senior director of the program. The VP for Quality and Compliance will provide necessary support in the development of this letter.	Managers, VP for Quality and Compliance
2. This notification letter must be written in simple language and include the following information: *What happened and when *What PHI was breached *Things that the person can/should do in response to the breach (i.e., monitor their credit) *What we're doing to find out how it happened *What we're doing to prevent it from happening again *What we're doing so that people aren't hurt by the breach *Who they can call with questions.	Managers
3. This letter needs to be hard-copy mailed to the last known address of the person whose information was breached unless the person prefers to receive this via email. If the person whose information was breached is deceased, we need to send the letter to the last known address of their next of kin.	Managers
4. If our contact information is out of date for fewer than 10 people, we can let them know in other ways, such as by phone. Any alternate communications must be documented in our Electronic Health Record.	Managers
5. If our contact information is out of date for more than 10 people, we are required to: *Put something about the breach on our webpage; OR *Put something out in the local media.	Managers, VP for Quality and Compliance

Both of these must include a toll-free number where people can call to find out if they were affected by the breach. The VP for Quality and Compliance will assist managers in this situation.	
6. For a breach involving more than 500 people, we are required to put something on local media regarding the breach. This has to occur within 60 days of when we first discovered the breach. We will work with Executive Leadership, Marketing and Communications, and legal counsel (as appropriate), to accomplish this.	VP for Quality and Compliance
7. Managers are also required to respond to the findings of the review or investigation and provide the following information: *Actions being taken to prevent recurrence of the breach *Information on any disciplinary actions take with staff	Managers
8. Managers should keep a copy of the letters for their records, but also send a copy to the VP for Quality and Compliance to include with the compliance case record, and for the FTC notification which will need to occur.	Managers
9. The compliance case will be presented to and reviewed by the Internal Compliance Committee.	VP for Quality and Compliance
10. For a case involving more than 500 people, we are required to notify the FTC within 60 days of when we first discovered the breach.	VP for Quality and Compliance
Manager responsibilities:	
1. Managers are responsible for setting an example for staff on keeping PHI secure.	Managers
2. Managers should have a good working understanding of this procedure and their role in it.	Managers
3. Managers have a responsibility to respond quickly and effectively if they believe that a breach has occurred.	Managers
4. Managers should reach out in a timely manner for support if needed to fulfill their obligations under this procedure.	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
4. Responsible for ensuring that breaches are PHI are handled within the requirements of the law.	VP for Quality and Compliance

Document revision record:

Revision Date	Release Date	Reason for change	Approver
8/4/17	8/4/17	Reasons for change not documented	P Dancer
11/20/18	11/20/18	Reasons for change not documented	P Dancer
1/27/21	1/27/21	Transitioned to new procedural format and fleshed out responsibilities	P Dancer
1/24/23	2/24/23	Revised PrecisionCare to Electronic Health Record; Corrected Typos; Activated the risk assessment link	ICC
1/25/24	1/25/24	Clarified need to respond to improper disclosure not just breach; added that level of risk includes type of PHI involved; clarified parties to assist with a large breach	ICC

HIPAA HITECH Breach Notification
Risk assessment

This assessment is used to determine if a disclosure of protected health information (PHI) meets the HIPAA HITECH requirements for breach notification.

Incident #: Date Reported: Involved Program(s):

Date Discovered: Notification deadline:

Discovering party/title: Reporting party/title:

Did the situation involve a Business Associate?: Yes If yes, please describe:

Name(s) of person(s) served:

Number of people served involved:

Information used/disclosed:

Recipient(s) of information:

Party responsible for the use/disclosure and title:

Brief description of the use/disclosure:

Based on the following assessment, is there a high probability that the PHI has been compromised? Yes

Rationale for determination:

Preliminary Assessment:

1. Is the information involved in the breach protected health information (PHI)? Yes
   If No, then STOP. No breach has occurred.

2. Was the information encrypted or shredded at the time of the disclosure? Yes
   If Yes, then STOP. No breach has occurred.

3. Was this unintentional or good faith access or acquisition made by a member of The Arc's workforce (i.e., employee, volunteer, contractor, student or intern)? Yes
   If Yes, then STOP. No breach has occurred.

4. Was this an inadvertent disclosure by an Arc workforce member to another Arc workforce member? Yes
   If Yes, then STOP. No breach has occurred.

5. Is it reasonable to assume that the recipient could not have retained the information? Yes
   If Yes, then STOP. No breach has occurred.

6. Is data limited to the limited data set that does not include DOBs or zip codes? Yes
   If Yes, then STOP. No breach has occurred.

If you did not STOP at the above questions, please complete the secondary assessment.

Secondary Assessment:

1. Given the type of information improperly used or disclosed, what specifically makes it PHI?

2. Level of risk associated with the type of PHI involved (per the criteria below): Low Risk

    a. Low risk: Limited data set; PHI breached does not include health information (only the following: name, address, city, state, telephone number, tax number, e-mail address, admission/discharge dates, service dates, date of death
    b. Moderate risk: Non-sensitive PHI which may include information about treatment, diagnoses, service, medications, etc.
        i. It's important to evaluate carefully in the context of the breach to determine the true risk for the person. In some cases, the true risk may be high.
        ii. Note: some diagnoses automatically make the risk high. These include (but may not be limited to) HIV, substance use disorder or mental health diagnoses.
    c. Highest risk:
        i. Information defined by the Identity Theft Protection act which includes the person's first name or first initial and last name in combination with any of the following:
            1. Social security or employer taxpayer ID Numbers
            2. Driver's license, state ID card or passport numbers
            3. Checking account numbers
            4. Savings account numbers
            5. Credit card numbers
            6. Debit card numbers
            7. PIN codes as defined in GS 14-113.8(6)
            8. Electronic identification numbers, e-mail names or addresses
            9. Internet account numbers or internet identification names
            10. Digital signatures
            11. Any other numbers or information that can be used to access a person's financial resources
            12. Biometric data such as fingerprints
            13. Passwords
            14. Parent's legal surname prior to marriage
        ii. Sensitive diagnostic information (as described above in bullet 2. b.)

3. Given the nature of this PHI, is there a likelihood that the information accessed or disclosed could be used in a manner adverse to the individual or otherwise further the recipient's own interests? Yes

    Please explain:

4. If the PHI did not include any direct identifiers, is there a likelihood that the recipient could correctly figure out who the individual(s) is(are)? NA

    Please explain:

5. Was the recipient of the PHI a workforce member of a covered entity? Yes

    Please describe:

6. Was the information retrieved or returned before it could be accessed by the recipient? Yes

    Please explain:

7. Did the recipient respond to the improper use or disclosure in a way that mitigates the likelihood that the PHI has been compromised? Yes

If yes, please check the appropriate box below:

- ☐ Recipient notified The Arc immediately of the disclosure
- ☐ Recipient indicated that the information has been secure or otherwise protected from further access or disclosure.
- ☐ Recipient indicated that the information has been shredded
- ☐ Recipient indicated that the information has been secured pending direction from The Arc of Monroe County
- ☐ The PHI was not used/disclosed by the recipient past the initial disclosure (e.g., the PHI was reasonably controlled).
- ☐ The recipient is a workforce member for a covered entity (and therefore is obligated as part of his/her responsibilities to protect the privacy and security of the information)
- ☐ The recipient mailed back or otherwise returned the improperly disclosed information to The Arc
- ☐ Other:

Please explain if necessary:

Date of internal compliance committee review:

Date closed: