WHAT WE NEED TO DO IF UNSECURED PHI GETS BREACHED

STANDARD:

The Arc wants to make sure that unsecured PHI is kept secure. Unsecured means that that if someone sees it, they can read it and understand what it says or means. To be secured:

- PHI needs to be encrypted. This means that if someone gets it, the letters are all scrambled and can't be understood.
- PHI needs to be shredded.

A breach means that someone got access to PHI that they shouldn't have. This could happen if we send PHI to the wrong person. It can also happen if we leave PHI lying around where people can see it. It can happen if PHI gets stolen from us, too. If we think PHI was breached, there are certain people we need to tell. That's what this policy is about.

When a breach happens, we look at what kind of PHI it was, who got it, and what they did with it afterwards. That will help us decide if the PHI was "compromised". This means that someone could use it in a way that hurts the person. Examples: using their name and social security number to open a credit card account. It might also mean pretending to be the person or using their health insurance information to get health care. We look at all these things and then decide if we believe there really was a breach or not.

There are some things that are automatically NOT a breach:

- If an Arc employee looks up the wrong person and sees their PHI, that would not be a breach. Example: a staff person wanted to look up John Smith in PrecisionCare. On accident, they looked up Tom Smith. They didn't realize it until they had seen some PHI about Tom.
- If one Arc employee accidentally sends PHI to another Arc staff person and they shouldn't have. Example: a staff person thought that Sue Jones (Arc Staff) worked with someone we support. They send information about that person to Sue Jones when she doesn't really work with them.
- If information is shared in front of someone who would not be able to understand or remember the information. Example: a staff person shares PHI with another staff in front a someone who is sound asleep. Since they are asleep, they could not understand what was being said.

PROCEDURE:

1. Staff needs to tell a manager as soon as they think a breach might have happened. It should happen right away. It has to happen within 24 hours.
2. A possible breach is "discovered" on the first day that ANY Arc staff person knows about it. This is important because if we really have a breach, we have to let people know in a certain amount of time.
3. Management will look at what happened and decide if they think it might really be a breach. They can always talk with the VP for Quality and Compliance to help decide.

4. If they think they do have a breach, they need to call the VP for Quality and Compliance. That needs to happen within 24 hours of when they think they have a breach.
5. If we really have a breach, there are some things managers need to do. They need to tell the people whose information was breached that it happened. They have to do this as soon as possible, but within 60 days of when we knew we had a breach.
6. The only time we can take longer is if the police tell us to wait. They might do that to make sure they can do their investigation right. We would need to get that in writing. They would also have to tell us in writing why they want us to wait. If they ask us verbally to wait, we can only wait 30 days unless we get something in writing in those 30 days. If we don't, at the end of the 30 days we have to tell people.
7. When managers tell people about the breach, they have to tell them:
    a. In writing
    b. What happened and when
    c. What PHI was breached
    d. Things the person should do so they aren't hurt by the breach
    e. Things we're doing to find out what happened
    f. Things we're doing to keep it from happening again
    g. Things we're doing so people aren't hurt by the breach
    h. Who they can call with questions
    i. This has to be in simple plan language that is easy to understand.
8. These need to be sent to the last known address we have for the person. If the person is OK getting an email instead we can do that.
9. We need to keep copies of whatever we send out. The program where the breach happened should keep those.
10. Managers also need to write down what PHI was breached on the "accounting of disclosures" form. Please see that policy for more information.
11. If the person whose information was breached is dead, we need to send this to their next of kin if we have their address.
12. If our contact information is out of date for fewer than 10 people, we can let them know in other ways. This can include phone.
13. If our contact information is out of date for more than 10 people, then we have to:
    a. Put something on our webpage OR
    b. Put something in the local media.
14. Both of these have to include a toll-free number where people can call. This number has to be active for at least 90 days. People can call to find out if their information was breached.
15. If we think someone needs to know right away about a breach, then we can call them or tell them in person. We still have to send the letter out even if we do that.
16. If the breach affects more than 500 people, we have to send letters out AND we have to put something on the local media about the breach. This also has to happen within 60 days of when we know we have a breach.
17. If a breach affects more than 500 people, we also have to tell the Federal Health and Human Services Department about the breach. We have to do this as soon as possible but within 60 days.

18. Business associates need to let us know if they think they have a breach. Please see the policy on business associate agreements for more information.
19. We will keep any information about breaches for at least 6 years from the date of the breach.

Effective date:
9/23/09
8/4/17
11/20/18