



AgeWell Services of West Michigan	
Policy Name: HIPAA-Confidential Information Protection Policy	
Policy No. PS 1.2	Effective Date: 5/30/19
Approved: <i>Kristen M. Collee</i>	Last Revised:

SCOPE and POLICY: It is the intent of AgeWell Services (AWS) to ensure responsible data security and to abide by HIPAA federal law that was instituted to assist individuals with managing their Personal Health Information (PHI) obtained by various businesses in the course of providing services to individuals. This law also limits what a service provider can do with PHI.

What is considered Personal Health Information (PHI)?

- First or last name
- Address
- Employer
- Relative's names
- Date of birth
- Phone and fax numbers
- E-mail address
- Social Security Number
- Member, certificate or account numbers
- Photos or fingerprints
- Service or billing codes

Any other information which may identify the individual: reason participant is in a program, medications the participant is taking or has taken, or information regarding past health conditions

What is considered a breach of PHI information?

The unauthorized acquisition, access, use or disclosure of unsecured PHI which compromises the privacy of such information for the participant/individual.

Examples of a breach: Participant record documents left in the view of public or visitors, papers containing PHI found offsite-such as in trash (not shredded) or after a vehicle is involved in a break-in or accident, papers falling out of a brief case or bag, or mailing participant information to the wrong address.

How can I protect PHI information?

- Never leave route sheets or other paperwork lying out on the car seat
- If you are unable to turn your paperwork in the same day, have a secure place to keep it until it can be turned in
- If paperwork is misplaced, call the office immediately
- Do not share computer passwords with anyone
- Always use a password protected screensaver set on 5 minutes or less

PROCEDURE: Team Members of AWS will, at all times respect the confidentiality of participants PHI and will endeavor to ensure the collection, storage and disclosure of PHI remains confidential. Team Members will be sure to thoroughly follow the [Agency Acceptable Use HR Policy 1.8](#) ensuring information transmitted via technology is secure and not susceptible to a PHI breach.

ENFORCEMENT: All suspected breaches will be investigated promptly by the Executive and/or Associate Director, and will involve swift recovery of information (if applicable). A breach of PHI information is subject to disciplinary action including and up to termination of employment.

REFERENCES:

[Acceptable Use Policy](#)

[Discipline Policy](#)