Privacy and Security Standards

Missouri Association of Area Agencies on Aging (MA4)

The Missouri Association of Area Agencies on Aging (MA4) does not collect, store, transfer or dispose of Personally Identifiable Information (PII). MA4 takes the privacy and security of Personally Identifiable Information (PII) very seriously. Toward that end, we have implemented procedures in relation to the implementation of the Navigator grant and our role in assisting consumers with the Missouri Health Insurance Marketplace. MA4 requires its Navigators and subcontractors to implement the following privacy and security principles.

These safeguards include but are not limited to:

- No person shall disclose any record by any means of communication to any person or another agency without a written request or prior written consent of the individual to whom the record pertains. PII will not be shared with persons who are not authorized to receive it.
- All employees/volunteers who will handle PII are subjected to screening that includes a criminal background check, licensure verification (when required), and exclusion list validation.
- Access to electronic PII is granted using the principle of least privilege.
- Computer systems containing PII are encrypted.
- Antivirus software is updated to prevent malware installation/data loss.
- Compliance processes are in place to report and quickly address suspected security breaches.
- Full back-up systems are in place and functioning.
- Request for Assistance/Health Insurance Marketplace Counseling Consent Forms shall be secured in a locked file or password protected digital file for six (6) years following the ending date of the contract.

Collection of PII:

- Navigators will advise all consumers of their right to consent or refuse use of data about them.
- If requested, consumers may receive a copy of the consent form.
- Consumer Consent and Registration Forms will be maintained in a secure, locked container until transfer to data entry location.
- Electronically scanned copies will be stored in a secure, password-protected database.
- Data will be inputted into a secure, password-protected database.
- Navigators will ensure messages, faxes, and e-mails that contain personal information are properly marked and e-mail is encrypted.
- All records containing PII should be stored in locked filing cabinets or other secure containers to prevent unauthorized access.
- Electronic records must be password protected and be transferred via encrypted e-mail.

Transporting PII:

- Hand carrying:
    - Use a cover sheet or file folder to shield contents
- Postal Mail:

    - Use manila or white envelopes
    - Mark the envelope to the attention of the authorized recipient
    - Never indicate on the outer envelope that it contains PII
- Using email:
    - Password protect PII placed on shared drives, the Internet or the Intranet
    - Use encrypted e-mail
    - Do not send PII to a personal, home or unencrypted e-mail address
    - Announce in the opening line of the text (NOT the subject line) that PII is contained within

Disposal of PII:

- PII forms shall be destroyed after data entry.
- A disposal method is considered adequate if it renders the information unrecognizable or beyond reconstruction. Disposal methods may include:
    - Burning
    - Melting
    - Chemically decomposing
    - Pulping
    - Pulverizing
    - Shredding
    - Mutilating
    - Degaussing (erasing magnetic field or disc)
    - Deleting/emptying electronic "recycle bin"

Navigator Signature: _____ Date: _____

Supervisor's Signature: _____ Date: _____