MARKETPLACE
ASSISTER TOOLKIT

Standard Operating Procedures Manual for Assisters in the Individual Federally-facilitated Marketplaces
CONSUMER PROTECTIONS: PRIVACY AND SECURITY GUIDELINES

Table of Contents

CONSUMER PROTECTIONS: PRIVACY AND SECURITY GUIDELINES 1

A. Privacy & Security Guidelines 1

1. Personally Identifiable Information 1

2. Tips for Protecting PII 4

List of Exhibits

Exhibit 1—Common Consumer Questions About Assister Use of PII 4

Consumer Protections: Privacy and Security Guidelines

A. Privacy & Security Guidelines

When you help consumers apply for health coverage throughout the Marketplace, they may provide personal information to you. Consumers should be able to trust you to handle their personal information with care. Some of this information will be personally identifiable information (PII). The term "personally identifiable information" means information that can be used to distinguish or trace an individual's identity. Another way to think about PII is that this information alone, or when combined with other personal information, can be linked to a specific individual. Examples of PII include the consumer's:

- Name
- Social Security Number (SSN)
- Date of birth
- Address
- Income
- Protected health information
- Tax information

In general, consumers should input their own information in an online or paper application unless a consumer asks for help typing or using a computer to learn about, apply for, and enroll in Marketplace coverage online. An assister may then use the keyboard or mouse but must follow the consumer's specific directions.

An assister must not log into a consumer's online Marketplace account, fill out the online or paper Marketplace application, or select a plan unless directed by the consumer. The consumer or the consumer's authorized representative must complete a consent form before the assister may access the consumer's PII.

1. Personally Identifiable Information

Review the guidelines in this section to understand your role in protecting consumer's PII and to be aware of situations in which you may come into contact with PII. Also review How to Obtain a Consumer's Authorization before Gaining Access to Personally Identifiable Information (PII) for more information on obtaining consumers' authorization prior to accessing their PII.

The guidance in this section summarizes and supplements privacy and security standards that are specifically listed or incorporated in your or your organization's agreement with CMS, as required under 45 CFR § 155.260(b), and in your agreement with your organization. In addition, CMS regulations require you to obtain a

consumer's authorization (also referred to in this document as consent) prior to accessing a consumer's PII (refer to SOP 1 – Receive Consent Before Accessing Consumer PII). You are allowed to access, keep, and use consumer PII to carry out your assister "authorized functions", which are listed in the privacy and security standards within the Cooperative Agreement to Support Navigators in Federally-facilitated Exchanges and which generally include the activities you are authorized under CMS regulations to perform in your role as an assister as well as for any other purpose for which a consumer has provided specific consent, consistent with applicable law. In the event that you encounter a consumer's PII, you must adhere to all applicable privacy and security standards.

Your responsibilities include:

- Knowing, understanding, and complying with the privacy and security standards in any grant, contract, or agreement between CMS and you and your assister organization and in the terms and conditions of any contract or agreement between you and your assister organization.
- Recognizing and protecting consumers' private information, including PII, and any other sensitive information that belongs to consumers.
- Informing consumers how their PII will be secured.
- Obtaining consumers' authorization (or consent) prior to gaining access to their PII.
- Maintaining a record of a consumer's authorization for at least six years (unless a different and longer retention period has already been provided under other applicable federal law) and informing consumer that they can revoke this authorization at any time.
- Providing consumers with a written privacy notice statement that has been developed by your organization (or ensuring that your organization has provided consumers with this privacy notice statement) prior to collecting PII or other information from them in connection with carrying out your assister duties. However, the privacy notice statement doesn't need to be provided to consumers prior to collecting their name, physical address, email address, or telephone number if that information is being used only to make future contact with the consumer to carry out an authorized function, such as setting up an appointment, or to send them educational information directly related to your authorized functions.
- Only sharing consumers' PII with other individuals or organizations as authorized by the terms and conditions of any grant, contract, or agreement between CMS and you and your organization; the terms and conditions of any contract or agreement between you and your assister organization; or with a consumer's express consent.

- Maintaining an account of any and all disclosures of PII, except for those disclosures that are necessary to carry out your authorized functions. Your accounting should contain the date, nature, and purpose of such disclosures and the name and address of the person or agency to whom the disclosure is made. You should retain the account for at least six years after the disclosure, or the life of the consumer's record, whichever is longer. This account must be made available to CMS or the consumer who is the subject of the record upon request. Disclosures of PII that have not been authorized by the consumer may be considered a privacy breach or incident depending on the circumstances.

You may come across consumers' PII when you:

- Obtain their authorization to provide assistance;
- Assist them with creating an account through the FFM;
- Assist them with the FFM eligibility application for health coverage; and
- Assist them with understanding how to file an FFM eligibility appeal.

Some request or collections of PII are prohibited, however. For example, you and your organization are not permitted to:

- Request or require a SSN, information regarding citizenship, status as a U.S. national, or immigration status for any individual who is not personally seeking coverage on an application.
- Request information from or concerning any individual who is not personally seeking coverage unless that information is necessary for the FFM eligibility application of another person seeking coverage. Such necessary information may include information on individuals who are in an individual's tax household or who live with an individual applying for coverage, including contact information, addresses, tax filing status, income and deductions, access to employer-sponsored coverage (ESC), familial or legal relationships, American Indian or Alaska Native status, or pregnancy status.
- Use consumers' PII to discriminate against them, such as by refusing to assist consumers who have significant or complex health care needs.

Exhibit 1 is a resource to answer common questions from consumers about assister use of PII in the Marketplace.

Exhibit 1—Common Consumer Questions About Assister Use of PII

Why might you ask for my personal information?	What will NOT happen with my personal information?
• To help you apply for health coverage through an FFM • To help you apply for programs to lower costs of health coverage • To help you identify qualified health plan (QHP) options available through an FFM • To schedule appointments with you • To provide assister services in a culturally and linguistically appropriate manner and in a manner that is accessible to persons with disabilities	• Information will not be used for purposes unrelated to the assister's authorized functions • Information will not be used for purposes to which a consumer hasn't consented

2. Tips for Protecting PII

Here are some tips that will help you protect consumer's PII.

2.1 Handling PII

- You are required to keep or store any copies of documents containing a consumer's PII only in a manner that is consistent with the privacy and security standards that apply to you. If you need to keep a consumer's document containing PII to carry out an authorized function, best practice is to keep a copy and return the originals to the consumer.
- You may use or disclose PII only to carry out your authorized functions or with a consumer's specific consent.
- If you send information that may contain PII to other individuals or organizations, you may do so only to carry out your authorized functions or with a consumer's consent and must do so in a manner that is consistent with the privacy and security standards that apply to you.

- You should not leave files or documents containing PII where others could inadvertently see them and secure any documents that contain PII before leaving your desk or workstation. As a best practice, pick up documents that contain PII promptly from printers and fax machines.
- When assisting consumers who will be mailing their PII (such as a hard-copy FFM application), advise them that it's a good idea to use an opaque envelope or container and, If possible, use a traceable delivery service.
- When assisting consumers who will be faxing PII, it's a good idea to double check that the recipient's fax number is correct and that someone is able to receive the faxed information promptly.
- Remind consumers they should keep their PII in a secure place that they will remember.
- If consumers mistakenly or accidentally leave behind PII at a facility or enrollment event, return it to consumers as soon as possible and store the PII securely until that time.
- If it is not possible to return PII to a consumer and the PII is not in the form of an original document such as an original Social Security card or government-issued identification card, you should consider destroying the PII and maintaining a record of its destruction. If the PII is in the form of an important original document like a Social Security card or government-issued identification card, we recommend that you return the document to the agency or entity that issued it and keep a record of its submission to that agency.
- Assisters should use email accounts, websites, and mobile devices in a manner consistent with their organization's implementation of the privacy and security standards when collecting, transmitting, or accessing PII.
- As a best practice, clear your web browser history after using your browser to access PII so that another person using the same computer and web browser does not inadvertently access the PII.
- Use passwords to protect electronic accounts that may contain PII as well as additional safeguards to protect electronic accounts, consistent with your organization's implementation of the privacy and security standards. Remind consumers to do the same.

2.2 Reporting a Breach of PII

- Your organization must have its own breach- and incident-handling procedures that are consistent with CMS's Risk Management Handbook that details the identification, response, recovery, and follow-up of incidents and breaches. These procedures must identify the designated Privacy Official for the organization (if applicable) and other personnel who are authorized or responsible for reporting and managing privacy and security incidents or breaches to CMS.

- You must comply with your organization's breach- and incident-handling procedures.
- Your organization's breach- and incident-handling procedures must address how to identify an "incident". An "incident" is the act of violating an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data, and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.
- If an incident occurs, you and tour organization should follow its policies and procedures to determine if PII is involved in the incident.
- If you discover that a potential incident or breach of PII has occurred, you should immediately report this to your organization's designated Privacy Official and any other person who has been identified as responsible for reporting or managing a breach of PII for your organization.
- Your organization must report any incident or breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within one hour of discovery of the incident or breach.
- In addition, your organization must complete a CMS Security Incident Report.
- You and your organization must cooperate with CMS in resolving any incident or breach and provide details regarding identification, response, recovery, and follow-up of incidents and breaches. Your organization must also make its designated Privacy Official or other authorized personnel available to CMS upon request.