MARKETPLACE
ASSISTER TOOLKIT

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

Version 8.0 November 2022. This information is intended only for the use of entities and individuals certified to serve as Navigators or certified application counselors in a Federally-facilitated Marketplace. The terms "Federally-facilitated Marketplace" and "FFM," as used in this document, include FFMs where the state performs plan management functions. Some information in this manual may also be of interest to individuals helping consumers in State-based Marketplaces and State-based Marketplaces using the Federal Platform. This document is intended only as a summary of legal requirements and to provide operational information and does not itself create any legal rights or obligations. All legal requirements are fully stated in the applicable statutes and regulations. This material was produced and disseminated at U.S. taxpayer expense.

Table of Contents

List of Exhibits

Consumer Protections: Privacy and Security Guidelines

A. Privacy & Security Guidelines

When you help consumers apply for health coverage through the Federally-facilitated Marketplace (FFM, or 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). PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Common examples of PII that you may collect, disclose, access, maintain, store, and/or use when helping consumers in the Marketplace include, but are not limited to, the examples listed in Exhibit 1.

Exhibit 1 - Common Examples of PII

Common Examples of PII	
• Name • Social Security Number (SSN) • Date and place of birth • Phone number • Home address • Email address	• Driver's license number • Mother's maiden name • Income • Medical, educational, financial, and/or employment information • Electronic or paper tax returns (e.g., 1040, 941, 1099, 1120, and W-2)

In the event that you encounter a consumer's PII, you must adhere to all applicable privacy and security standards. The guidance in this document summarizes and supplements privacy and security standards that are specifically listed or incorporated in your or your organization's agreement with the Centers for Medicare & Medicaid Services (CMS), as required under 45 CFR § 155.260(a), and in your agreement with your organization. These are included in the following:

- Navigators: Attachments H, I, and J of the 2022-2024 grant terms and conditions (T&Cs)

  Note: Navigators may **not** create, collect, handle, disclose, access, maintain, store, and/or use the PII (as defined in Attachment J of the T&Cs) of any consumers until they have drawn down funds and, in doing so, have accepted the terms and conditions of their award.

- Certified application counselors (CACs): Formal agreement between CMS and the CAC designated organization (CDO)

These privacy and security requirements are designed to make sure that:

- Consumers' information is accurate.
- Information is used only when necessary and relevant to the immediate activity.
- Consumers know and agree to all uses of information.
- Appropriate, swift action is taken when an incident or breach occurs.

- Confidentiality is protected to comply with all applicable laws and create trust between assisters and consumers.

You must be familiar with these requirements to make sure consumers' privacy is protected. Keep in mind that subgrantees, or organizations you contract with, must be held to the same standards regarding the use and disclosure of consumers' PII.

1. Privacy and Security Requirements

Before you begin helping consumers, there are important things you must do to follow FFM privacy requirements:

- Make sure your organization has appropriate policies and procedures in place for collecting, protecting, and securing all PII.
- Provide consumers with a privacy notice statement before you collect PII or other information from them. If your organization uses a paper or electronic form to gather or request PII from consumers, this statement may be included on that form.
- Clearly display the privacy notice statement on your organization's public-facing website if you use such a website to collect PII or other consumer information.
- Always obtain consumers' consent, or "authorization," from the consumer or the consumer's authorized representative before discussing or accessing their PII (for more information on obtaining consumers' consent, refer to Standard Operating Procedure (SOP) 1 – Receive Consent Before Accessing Consumer PII at Marketplace.cms.gov/technical-assistance-resources/sop-section-1.pdf).
- Let consumers know what PII you will collect, why it's collected, how you will use it, with whom the information can be shared, and what happens if they don't want to provide it.
- Only collect information that is necessary to perform authorized Marketplace functions and assist consumers unless they give you specific consent for additional uses.
- Inform consumers how their PII will be secured.
- Maintain an account of any and all disclosures of PII. 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, and assisters should inform consumers that they may request their records. Disclosures of PII that have not been authorized by the consumer may be considered a privacy breach or incident depending on the circumstances.

- Recognize and protect consumers' private information, including PII and any other sensitive information that belongs to consumers.
- Only share 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.

You must comply with all other applicable state and federal laws related to the privacy and confidentiality of PII. It's your responsibility to understand which privacy and security laws and regulations apply to your role in the FFMs and to fully comply with those laws. States may establish their own laws or regulations governing the activities of Marketplace assisters as long as those laws don't prevent the application of Title I of the Affordable Care Act (ACA). Several states have passed laws and implemented regulations that impose additional requirements on assisters.

2. Privacy Notices

Prior to collecting PII or other information from consumers in connection with carrying out your assister duties, you must provide the consumer with a written privacy notice statement (or ensure that your organization has provided the consumer with this privacy notice statement).

The privacy notice must be:

- Written in plain language.
- To the extent possible, provided in a manner that is accessible and timely to people with disabilities and people with Limited English Proficiency (LEP).

A privacy notice must contain, at a minimum, the elements listed in Exhibit 2.

Exhibit 2 - Minimum Privacy Notice Statement Elements

Minimum Privacy Notice Statement Elements	
• A description of the information to be collected • The purpose for which the information is being collected • The intended use(s) of the information • To whom the information may be disclosed, for what purposes, and how a record of any disclosures may be requested • What, if any, notice or opportunities for consent will be provided regarding the collection, use, or disclosure of the information	• How the information will be kept secure • Whether the information collection is voluntary or mandatory under applicable law • What the effects are if a consumer chooses not to provide the requested information • Consumers' privacy rights under state and federal law • Information on how to file complaints with CMS as well as the CAC or Navigator organization about the organization's activities in relation to the information collected

You are permitted to collect a consumer's name, mailing address, email address, or telephone number without first providing a written privacy notice statement if you are using this information solely to:

- Follow up with the consumer and conduct an authorized assister function, such as setting up an appointment.
- Send educational information to the consumer that is directly relevant to your authorized functions.

Your organization must review the privacy notice statement at least annually and revise as necessary, including after any change to the organization's privacy policies and procedures.

3. Handling Consumer PII

Consumers might ask why you need to discuss so much personal information with them when you help them apply for and enroll in coverage through the Marketplace. You should tell them that the Marketplace uses their PII to:

- Determine or assess eligibility for Marketplace coverage, Medicaid, and Children's Health Insurance Program (CHIP) coverage.
- Determine eligibility for programs to lower costs of coverage.
- Display qualified health plan (QHP) options.
- Process eligibility appeals, if applicable.
- Perform other authorized functions.

You may also come in contact with consumers' PII for other purposes for which the consumer provides their specific, written, informed consent. Assisters are permitted to create, collect, disclose, access, maintain, store, and/or use consumer PII after obtaining consumers' consent **only** to perform functions that they are authorized to perform as assisters in accordance with the terms and conditions for Navigators and the CDO-CMS agreement for CACs.

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.

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

- Request or require an SSN or information regarding citizenship, status as a U.S. national, or immigration status for any consumers who aren't seeking coverage for themselves on any application, unless the consumer has separately provided informed consent in writing for you to access this information.

- Request information from the applicant, authorized representative, or directly from any individual who is not seeking coverage for themselves, unless that information is needed for the Marketplace to determine an applicant's eligibility for enrollment in a QHP or an insurance affordability program. 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.
- Collect PII beyond what is necessary to perform your authorized functions without the specific, informed consent of the consumer.
- Use PII to discriminate against consumers, such as refusing to assist individuals who are older or who have significant or complex health care needs.
- Make cold calls, send unsolicited emails, or use other means of unsolicited direct contact for the purpose of providing application or enrollment assistance, unless:
    - You have a pre-existing relationship with a consumer.
    - You have complied with all other applicable state and federal laws.

Exhibit 3 is a resource to answer common questions from consumers about assister use of PII in the Marketplace.

Exhibit 3 - 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 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

4. Tips for Protecting PII

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

To protect consumers' PII, remember the following:

- 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 the 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.
- 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.
- If the consumer is physically present, make sure consumers take possession of their documents. Advise them that it's a good idea to use an opaque envelope or container and, if possible, use a traceable delivery service. However, assisters can provide postage materials and/or mail a paper application on a consumer's behalf as long as the consumer consents to the assister's retaining the application for this purpose. Assisters can add a specific consent to the Navigator or CAC model authorization form so that consumers can consent to having their application mailed on their behalf.
- Secure hard-copy consumer consent forms in a locked location. Don't leave forms unattended in a room or car.
- Restrict access so only authorized individuals have access to PII and/or are allowed in areas where PII may be accessed.
- Maintain employee awareness and train employees on how to safeguard PII.
- Make sure all scanning and copying equipment that may be used by consumers doesn't electronically retain copies of the images. 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.
- PII collected from a consumer – including name, email address, telephone number, application ID number, addresses, or other notes – must be stored securely.
- Dispose of PII in a manner consistent with FFM rules and retention requirements.
- 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.

- During consumer appointments, utilize private spaces to ensure privacy. If assisters are at an event and a private space is not available, create a space that is out of earshot to discuss private information with potential applicants. Also, use computer screen covers to help protect PII from the view of others.

To protect consumers' PII online and on devices:

- You can mention your role as an assister on Facebook, Twitter, and YouTube, but we recommend that you keep your references generic, such as letting people know the location where you'll be available for assistance. Don't mention any private information, such as consumers' specific names or medical conditions, without a consumer's specific, written consent to do so.

- 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.

  - Do not send or forward emails with PII to personal email accounts (e.g., Yahoo, Gmail).

  - Protect emails that contain PII (e.g., use encryption and password protections).

  - Do not upload PII to unauthorized websites (e.g., wikis).

  - Do not use unauthorized mobile devices to access PII.

  - Lock up portable devices (e.g., laptops, cell phones).

- Verify that "auto-fill" settings on your internet browsers are turned off.

- 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.

There are also other circumstances for which you must protect consumers' PII:

- If a consumer gives you contact information, such as by filling out a contact card or sign-up sheet at a community outreach event, this is considered consumer consent for future contact as long as the consumer was made aware the information might be used for future contact. In this case, follow-up contact with the consumer is permitted; however, you should obtain complete authorization for such

future contact, if and when you follow up with the consumer, in accordance with your organization's standard authorization procedures.

- Unless the consumer you are assisting specifically consents in writing, don't maintain additional client or demographic information beyond what is necessary to successfully perform authorized assister functions.
- You can keep certain client information, such as name, email address, or phone number, if the consumer consents and it's necessary for making or maintaining an appointment or carrying out authorized assister functions.
- CACs in FFMs may provide remote application assistance if such assistance is permitted by their CDO. CMS suggests that Navigator organizations and CDOs consider creating a specific plan for security when using screen-sharing applications and share that security plan with their assisters and consumers.

5. Privacy and Security Incidents

Security incidents are a potential threat to the confidentiality, integrity, or availability of PII. A security incident is the act (or attempt) of violating an explicit or implied security policy, which includes attempted or successful unauthorized access, use, disclosure, modification, or destruction of data or interference with system operations in an information system.

A privacy incident is a security incident that involves PII where individuals other than authorized users have access to PII. Privacy incident scenarios include:

- Losing encrypted or unencrypted electronic devices that contain PII (e.g., laptops, cell phones, disks, thumb drives, flash drives, CDs).
- Losing hard-copy documents containing PII.
- Sharing paper or electronic documents containing PII with individuals who aren't authorized to access it.
- Accessing paper or electronic documents containing PII without authorization or for reasons not related to job performance.
- Emailing or faxing documents containing PII to inappropriate recipients, whether intentional or unintentional.
- Posting PII to a public-facing website, whether intentional or unintentional.
- Mailing hard-copy documents containing PII to the incorrect address, whether intentional or unintentional.
- Leaving documents containing PII exposed in an area where individuals without approved access could read, copy, or move it for future use.

A breach is a privacy incident that poses a risk of harm to applicable individuals. The determination of whether a CMS privacy incident rises to the level of a breach is made exclusively by the CMS Breach Analysis Team (BAT). If you learn of a situation in which a consumer's PII has been compromised in any way, including an unauthorized person seeing or possessing the information or losing the records, the incident should be reported to CMS within one hour of discovery.

- Your organization must have its own breach- and incident- handling procedures that are consistent with CMS's Risk Management Handbook Chapter 08: Incident Response available at CMS.gov/files/document/rmh-chapter-08-incident-response.pdf 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.
- If an incident occurs, you and your 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 72 hours of discovery of the incident or breach.
- In addition, your organization must complete a CMS Security Incident Report available at CMS.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response-Appendix-K-Incident-Report-Template.
- 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.

If you don't protect PII or you disclose it inappropriately, you may cause harm to consumers, face disciplinary action by your organization, and be at risk for a civil money penalty (CMP) by the Federal Government. If you fail to protect consumers' information and/or purposefully disclose their PII for an unauthorized purpose, any of the following might occur:

- Consumers' identities may be stolen.

- You may lose consumers' trust because they are sensitive about sharing their personal information.
- You won't be in compliance with the standards of the FFMs.
- You may have to pay a CMP, or fine, of up to $25,000 per violation under the ACA.
    - HHS can impose a CMP if you knowingly and willfully use or disclose consumers' PII in any way that violates federal law and the FFM's privacy and security standards.
- When determining the amount of the CMP, HHS may consider factors such as the nature and circumstances of the violation and the actual or potential harm caused by the violation.
- You or your organization may be terminated from providing CMS-authorized assistance to consumers enrolling in health coverage through the FFMs.