Requirements and Best Practices for Assisters on Handling Personally Identifiable Information

This job aid provides guidance and best practices for Navigators, Certified Application Counselors (CACs), and Enrollment Assistance Personnel (EAPs) (collectively, assisters) when handling Personally Identifiable Information (PII).

Table of Contents

Overview....2
Handling Consumer PII....2
Privacy and Security Requirements....3
Protecting PII....7
PII Breaches and Security Incidents....9
Assister Best Practices....10
Additional Resources....12

Version 2.0. October 2024. This information is intended only for the use of entities and individuals certified to serve as Navigators, certified application counselors, or non-Navigator assistance personnel 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 material was produced and disseminated at U.S. tax filer expense.

Overview

Consumers may provide personal information to assisters when applying for health coverage through the Federally-facilitated Marketplace (FFM, or Marketplace). 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.

Each assister organization must refer and strictly adhere to the privacy and security standards that apply to them.[i] 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 it has drawn down funds and in doing so, has accepted the terms and conditions of their award.
- CACs: Formal agreement between CMS and the CAC designated organization (CDO).
- EAPs operate under a contracted assistance model.

Handling Consumer PII

When providing assister services to a consumer for the first time, assisters should first explain to the consumer their role as an assister and the privacy and security practices that they will take to ensure that the consumer's information is kept private and secure.

Assisters are permitted to create, collect, disclose, access, maintain, store, and use consumer PII only to perform functions that they are authorized to perform as assisters in accordance with the T&Cs for Navigators, CDO-CMS agreement for CACs, or contract for EAPs. Consumers must have an opportunity to access, inspect, and/or correct their PII if they make a request to do so.

Types of PII

A comprehensive list of types of PII that assisters might encounter and that they are authorized to access and use is provided in the privacy and security standards that apply to an organization's agreement or contract with CMS or grant terms and conditions, as applicable.

Common examples of PII include, but are not limited to:

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

Use of PII

PII is needed and used by the Marketplace to determine or assess consumers' eligibility for health coverage and programs to lower their costs through the Marketplace, as well as to identify available coverage options for all consumers. Assisters might also encounter PII as they help consumers select among various coverage options and enroll in coverage. As they assist consumers who are applying for and enrolling in coverage through the Marketplace, they will likely encounter PII when assisting consumers with:

- Creating a Marketplace account
- Completing and submitting an application for health coverage
- Assessing options for lowering costs of health coverage
- Selecting and enrolling in a qualified health plan (QHP)

Assisters may also come into contact with consumers' PII for other purposes for which the consumer provides their specific, written informed consent.

Privacy and Security Requirements

Before assisters begin helping consumers, there are important requirements and prohibitions for maintaining FFM privacy requirements as summarized in Exhibit 1. (Additional details about the items are presented in subsequent sections of this job aid).

Exhibit 1 - Privacy Requirements and Prohibitions

Requirements for Using PII	Prohibitions on Using PII
▪ Make sure your organization has appropriate policies and procedures in place for collecting, protecting, and securing all PII.	▪ Don't request information about a person's status as a citizen, national, or immigrant if that person is not seeking coverage for himself or herself on any eligibility application.
▪ Provide consumers with a Privacy Notice Statements 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.	▪ Don't request an individual's Social Security Number (SSN) if he or she is not seeking coverage for himself or herself, unless information about the individual's income is necessary to determine the applicant's household income.*
▪ 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.	▪ Don't use someone's PII to discriminate against them, such as by refusing to assist individuals who are older or have significant or complex health care needs.[ii] ▪ Note, however, that CAC organizations that are federally funded to provide services to a specific population, such as a Ryan White HIV/AIDS program or an Indian health provider, may continue to limit their services to that population as long as they do not discriminate within that specific population.
▪ Always obtain consumers' consent, or "authorization," before discussing or accessing their personal information.	▪ Don't request information about a person's status as a citizen, national, or immigrant if that person is not seeking coverage for himself or herself on any eligibility application.
▪ Let consumers know what personal information 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.	

*Note: an individual is not required to provide his or her SSN if he or she is not applying for coverage for himself or herself, but if the individual's income is included in the applicant's household income, providing this information can help speed up the verification process.

Assisters should be familiar with two important documents that they must use to comply with privacy standards: the **Privacy Notice Statement** and the **Record of Authorization**. Depending on an assister organization's policies and procedures, the record of a consumer's consent might be a completed consent form.

Privacy Notices

Prior to collecting PII or other information from consumers in connection with carrying out assister duties, assisters must provide the consumer with a written privacy notice statement (or ensure that their organization has provided the consumer with the most current privacy notice statement). The privacy notice statement must also be prominently and conspicuously displayed on the Recipient's public facing website, if applicable, if the Recipient will gather or request PII or other consumer information through that website.

The privacy notice statement must be written in plain language and, to the extent possible, provided in a manner that is accessible and timely to people with disabilities and people with Limited English Proficiency (LEP). The Privacy Notice Statement must explain how consumers can file a complaint with CMS and an assister organization related to an assister and/or assister organization's activities with respect to the PII. Organizations 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. A privacy notice statement must contain, at a minimum, the elements listed on the table 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 information ▪ How the information will be secured while in the possession of the Recipient or its Workforce or agents (sub-recipients)	▪ 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

Consumer Record of Authorization

Before gaining access to consumers' PII, assisters must obtain a consumer's authorization. Assisters are required to:

- Make sure consumers are informed of the assister's functions and responsibilities before providing assistance;
- Make sure consumers provide authorization by completing and signing a written form before obtaining access to a consumer's PII, and let the consumer know they can revoke that authorization at any time; and
- Maintain a record of the authorization for no less than six years, unless a different and longer retention period has already been provided under other applicable law.

CMS provides model authorization forms for CACs (English and Spanish), EAPs (English and Spanish), and Navigators (English and Spanish). However, an assister organization is free to develop its own form or procedures as long as the consumer's consent includes certain elements. Exhibit 3 provides a list of minimum consumer authorization form elements.

Exhibit 3 - Minimum Consumer Authorization Form Elements

Minimum Consumer Authorization Form Elements	

▪ Acknowledge that the consumer received information about Navigator and CAC roles and responsibilities. A list of roles and responsibilities. A list of roles and responsibilities is contained in "Attachment A" of the authorization forms
▪ Definitions of terms
▪ Authorizations:
  ▪ General consent to access and use the consumer's PII to carry out your Marketplace functions and responsibilities
  ▪ Specific consent(s) to obtain the consumer's PII for other purposes
  ▪ Additional information about the Navigator's or CAC's use of consumer PII
	▪ Exceptions or limitations to consents, including an acknowledgement that the consumer may revoke any part of the authorization at any time, as well as the description of any limitations that the consumer wants to place on your access to or use of the consumer's PII
	▪ Include an expiration date or event, unless effectively revoked in writing by the consumer before that date or event
	▪ Additional information about the Navigator's or CAC's use of consumer PII
	▪ Signature and space for consumer to provide contact information for follow-up, if desired

Assisters must keep a record of the consumer's authorization, which could include the authorization form used by their organization. At a minimum, the record of the authorization must include the following:

- The consumer's name and (if applicable) the name of the consumer's legal or Marketplace authorized representative
- The date the authorization was given
- Assisters name, or the name of the assister to whom authorization was given
- Notes regarding any limitations placed by the consumer on the scope of the authorization
- Notes recording all acknowledgments and consents obtained from the consumer
- If any changes are later made to the authorization, including if and when a consumer revoked the authorization, or any part thereof.

Protecting PII

Assisters and assister organizations must ensure that consumers' PII is protected with reasonable safeguards to ensure its confidentiality and prevent unauthorized or inappropriate access, use, or disclosure. Assister organizations must establish safeguards to ensure that:

- PII is only used by or disclosed to those authorized to receive or view it.
- PII is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information.
- PII is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law.
- PII is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with record retention requirements under an assister organization agreement with CMS or grant terms and conditions, as applicable.
- Assisters and their organizations must monitor, periodically assess, and update the security controls and related system risks to ensure the continued effectiveness of those controls.
- Assisters and their organizations must secure electronic safeguards (such as encryption software) when transmitting PII electronically.

Assisters should also remind consumers that they should keep their PII locked and in a safe place, or if stored electronically, protected by passwords that they will remember.

Exhibit 4 lists best practices for protecting PII in a variety of situations.

Exhibit 4 - Methods of Protecting PII

In person	Electronic	Paper
▪ Make sure consumers take possession of their documents. (If consumers mistakenly or accidentally leave behind PII at a facility or enrollment event, store the documents in a safe, locked location, and return PII to consumers as soon as possible.) ▪ Use private spaces when providing application and enrollment assistance. ▪ Secure hard-copy consumer authorization forms in locked filing cabinets or within locked offices where the paper filing system is maintained. ▪ Don't leave files or documents containing PII or tax return information unsecured and unattended. ▪ Restrict access to PII. ▪ Make sure all scanning and copying equipment that consumers may use doesn't electronically retain copies of the images. ▪ Dispose of PII in a manner consistent with FFM rules and retention requirements.	▪ Don't send or forward emails with PII to personal email accounts (e.g., Yahoo, Gmail). ▪ Protect emails that contain PII (e.g., encryption). ▪ Lock up portable devices (e.g., laptops, cell phones). ▪ Do not use unauthorized mobile devices to access PII. ▪ Do not upload PII to unauthorized websites (e.g., wikis). ▪ Clear web browser history and disable auto-fill settings on your web browser. ▪ All computer equipment, including mobile devices should have a password-protected login screen that will not allow access to files without the proper, secure password. The use of screen covers can help protect PII from the view of others.	▪ Encourage consumers to verify mailing addresses before they send forms. ▪ Always return originals or copies of official documents that contain a consumer's PII to consumers. ▪ Only make or retain copies of consumers' official documents if necessary to carry out required duties. ▪ Do not leave files or documents containing PII (including tax return information) unsecured and unattended on desks, printers, fax machines, personal computers, phones, or other electronic devices. ▪ If in hard copy, PII must be stored securely such as in locked filing cabinets or in locked offices where the paper filing system is maintained.

PII collected from the consumer, including name, email address, telephone number, application ID number, addresses, or other notes must be stored securely.

Keeping notes might be necessary to perform effective application and enrollment assistance for that consumer. For example, a consumer's case may require an assister to research their specific questions and follow up with them at a later appointment. If a consumer provides a general consent for an assister to gain access to that consumer's PII, they are permitted to keep notes linked to his or her individual situation, unless the consumer specifically limits his or her consent to prevent them from doing so. If an assister writes down any quick notes for their own reference during the phone call with a consumer but do not intend to keep those notes, the assister should shred the notes as soon as they complete the call. It can be helpful to have a supply of manila folders to hand to consumers with their documents inside. This helps them keep track of their documents in one place and shields the content of the documents from view.

PII Breaches and Security Incidents

Assister organizations must implement and comply with policies and procedures to handle PII breaches and security incidents consistent with CMS' Risk Management Handbook Chapter 8: Incident Response.

A breach is defined by OMB Memorandum M-17-12 (January 3, 2017), and means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for anything other than an authorized purpose.

Incident, or security incident, means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

An Assister and their organization must implement breach and incident handling procedures that are consistent with CMS' Incident and Breach Notification Procedures and memorialized in their organization's own written policies and procedures. Such policies and procedures would:

- Identify an organization's Designated Privacy Official, if applicable, and/or identify other personnel authorized to access PII and responsible for reporting and managing Incidents or Breaches to CMS.
- Address how to identify Incidents.
- Determine if personally identifiable information (PII) is involved in the Incidents. If in doubt, an assister must reach out to the CMS IT Service Desk at CMS_IT_Service_Desk@cms.hhs.gov
- Require all members of Recipient's Workforce to report all potential Incidents or Breaches to Recipient.

- Require reporting 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.
- Require the completion of the CMS Security Incident Report, which may be found at CMS.gov/about-cms/information-systems/privacy/incident-response.
- Provide details regarding the identification, response, recovery, and follow-up of Incidents and Breaches.
- Require the Recipient's Designated Privacy Official and/or other authorized personnel to be available to CMS upon request.

Issues an assister should report include:

- Lost, stolen, or misplaced records containing PII
- Unauthorized personnel seeing or possessing PII
- Lost, stolen, or misplaced electronic devices (e.g., tablets or laptops) that contain consumer PII.

Assister Best Practices

Consumers may have questions about the use of PII in the Marketplace. Exhibit 5 provides some common answers to these questions.

Exhibit 5 - Common Consumer Questions About Uses of PII

Why might you ask for 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 the 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 purpose unrelated to the assister's authorized functions ▪ Information will not be used for purposes to which a consumer hasn't consented

Best practices related to handling PII include:

- Prior to obtaining access to consumers' PII, develop and follow standard consumer authorization procedures that are appropriate for the nature of the work. For example, if an organization assists individuals over the phone, such procedures might include developing a verbal script and process to document and retain a consumer's oral authorization.
- Develop a checklist for assisters to use when providing assistance to a consumer for the first time. This plan will allow assisters to be sure all consumers provide their authorization (such as by signing an authorization form or orally consenting) before the session begins.
- Develop a standard operating procedure to document instances where a consumer withdraws or limits their authorization to access their PII.
- If a consumer has provided a general authorization to permit access his or her PII to provide assistance, as well as his or her preferred contact information, assisters may keep their name and contact information to set up appointments or to follow up with the consumer at a later date on application or enrollment issues.
- Preferred contact information can be documented at the same time that consumer authorization is obtained, consistent with an organization's standard consumer authorization procedures.
- Ask consumers if they have any questions about the information and/or form you have shared with them and be sure they understand your answers. It's a good idea to have the consumer verbally confirm that they understand what you have told them before they sign the form.
- Answer consumers' questions about the privacy and security of the PII they share with you. If needed to answer consumers' questions, refer to the model consumer consent form; your organization's Privacy Notice Statement; and the terms and conditions of your Navigator organization's grant or the agreement between you and your CAC organization and/or or your CAC organization's agreement with CMS.
- Consumers can access the FFM Privacy Policy for more information pertaining to PII.

Additional Resources

- Obtaining Consumer Authorization and Handling Consumers' Personally Identifiable Information (PII) in the Federally-facilitated Marketplace (FFM) webinar
- Requirements and Best Practices for Assisters on Providing Remote Consumer Assistance Guidance job aid
- Please also refer to, as applicable to your type of assister, the 2023-2024 Navigator Terms and Conditions, the most recently approved CDO-CMS agreement or EAP contracted assistance model.
- Centers for Medicare & Medicaid Services (CMS): Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- Internal Revenue Service (IRS) Publication 1075: Tax Information Security Guidelines For Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information (Jan. 2014)
- OIG Fraud Hotline
- Federal Trade Commission (FTC): Submission of Fraud Complaint

---

[i] Ecfr.gov/current/title-45/subtitle-A/subchapter-B/part-155/subpart-C/section-155.260 Marketplace Privacy and Security Standards at 45 CFR 155.260; any applicable privacy and security standards set forth in agreements, in accordance with §155.260

[ii] Ecfr.gov/current/title-45/subtitle-A/subchapter-B/part-155.210