CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Obtaining Consumer Authorization and Handling Consumers' Personally Identifiable Information (PII) in the Federally-facilitated Marketplace (FFM)

October 2024

This information is intended only for the use of entities and individuals certified to serve as Navigators, certified application counselors, enrollment assistance personnel or non-Navigator 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.

CSG-202410

Agenda

- Overview of Assister Privacy and Security Guidelines and Requirements
- General Assister Privacy and Security Requirements
- Privacy Notice Statement
- Obtaining Consumer Authorization Before Gaining Access to PII
- Consumer Authorization Requirements and Model Authorization Forms
- Consumer Scenarios
- Prohibited Requests for Collections or Uses of PII.
- Best Practices for Handling PII
- PII Breaches and Security Incidents
- Additional Resources

Assister Privacy and Security Requirements

- Navigators, Certified Application Counselors (CACs), and enrollment assistance personnel (EAPs) are collectively referred to as assisters throughout this presentation.
- Each assister organization must refer and strictly adhere to the privacy and security standards that apply to them. 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.

What is 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 assisters may collect, disclose, access, maintain, store and/or use when helping consumers in the Marketplace 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)

When Assisters May Come in Contact With PII

- You will likely come into contact with consumers' PII each time you help them with the following:
  - Creating a Marketplace account
  - Completing the eligibility process and submitting an application for coverage
  - Assessing options for lowering costs of coverage
  - Enrolling in a qualified health plan (QHP)
- You may also come into 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 T&Cs for Navigators and CDO-CMS agreement for CACs.

General Assister 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," before discussing or accessing their personal information.
- 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.

Privacy Notice Statement

- 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 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 your organization related to your and/or your organization's activities with respect to the PII.
- 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.

Privacy Notice Statement (Cont.)

A privacy notice statement must contain, at a minimum, the elements listed in this table.

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 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.

Obtaining a Consumer's Authorization Before Gaining Access to PII

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.

CAC, EAP, and Navigator Model Authorization Forms

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

- At a minimum, a **consumer's authorization** for obtaining consent includes the following elements listed in this table.

Minimum Consumer Authorization Form Elements	
▪ Acknowledge that the consumer received information about Navigator and CAC 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

CAC, EAP, and Navigator Model Authorization Forms (Cont.)

- The additional information section, among other things, specifies that the assister:
  - Will ask the consumer only for the minimum amount of PII necessary to help perform functions that they are authorized to perform as assisters.
  - Will ensure that the consumer's PII is kept private and secure and will follow privacy and security standards.
  - May follow up about applying for or enrolling in coverage after first meeting with the consumer if consumers choose to provide their contact information.
  - Might share the consumer's PII if referring the consumer to another source of help with the consumer's permission.
  - Will provide the consumer with copies of the completed authorization form and the Navigator's, EAP's, or CAC's roles and responsibilities.

Maintaining a Record of Authorization

- You must keep a record of the consumer's authorization, which could include the authorization form used by your 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
  - Your 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

Getting Consumer Authorization for Obtaining PII: Scenario #1

Scenario 1: Assisting a Homebound Consumer over the Telephone or Computer

You are assisting a consumer remotely over the phone or computer and need to obtain their authorization.

- You may obtain the consumer's authorization by reading them your organization's standard written authorization form or a script that contains, at a minimum, the required elements summarized above.
- You must record in writing that the consumer's authorization was obtained. The record of the authorization must include, at a minimum, the required elements summarized above.
- We strongly recommend that you create a record of the authorization as it is being provided, and then read back the content of the record to the consumer once it is complete so that the consumer can confirm that the record is accurate and complete, and correct it if it is not. We also strongly recommend sending the consumer a copy.

Getting Consumer Authorization for Obtaining PII: Scenario #2

Scenario 2: Outreach Events with Sign-up Sheets for Follow-up

Your assister organization is participating in an outreach or enrollment event. The organizers would like to create a sign-up sheet so that consumers who desire to receive a follow-up contact from a participating assister organization can leave their names and contact information.

- You may use a sign-up sheet to collect a consumer's name and contact information (i.e., mailing address, email address, telephone number) as long as you make clear on the sign-up sheet (and orally, if appropriate) that by providing their name and contact information, they are consenting to being contacted for application and enrollment assistance.
- Example: "By signing up, you agree that it is okay for an assister to contact you to help you with health care coverage and/or the Marketplace."

Getting Consumer Authorization for Obtaining PII: Scenario #2 (Cont.)

Scenario 2: Outreach Events with Sign-up Sheets for Follow-up (cont.):

- Any PII collected on the sign-up sheet should be kept private and secure and accessed only by staff who need it to carry out required duties. Any forms that are collected which include any PII need to be retained in accordance with the record requirements stated earlier.
- The privacy notice statement must be in writing and must be provided on, or simultaneously with, any electronic and/or paper form the Recipient will use to gather and/or request PII or other information from Consumers.
- 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.

Getting Consumer Authorization for Obtaining PII: Scenario #3

Scenario 3: Consumer makes initial contact and shares PII

You or your assister organization may receive a direct phone call, voicemail, or email from a consumer requesting your services as an assister. This communication will likely disclose the consumer's PII.

- If a consumer directly contacts you or your organization for assistance and provides their PII, you should still obtain a complete authorization from the consumer the next time you follow up with or meet in person with the consumer.
- Any PII collected during or by means of the initial contact must follow the requirements for maintaining authorization records discussed above and must be maintained privately and securely. Access to it should be given only to staff who need it to carry out required duties.

Getting Consumer Authorization for Obtaining PII: Scenario #4

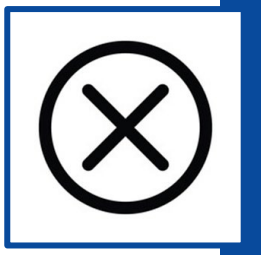
Scenario 4: A third party makes initial contact and shares consumer's PII

You might obtain access to a consumer's PII through a third party (for example, someone who is not you, your assister organization, or the consumer). The third party might share the consumer's PII without the consumer being present, which should raise concerns that the consumer had not authorized the third party to share their PII with you.

- Generally speaking, you are permitted to follow up with the consumer if the third party who contacts you confirms that they obtained the consumer's consent to share the consumer's PII with you or your organization so you can contact the consumer.
- Any PII collected by means of a third party should follow the requirements for maintaining authorization records discussed above.

Prohibited Requests for Collections or Uses of PII

- When using consumers' PII, assisters cannot:
  - Request information regarding citizenship, status as a national, or immigration status for any consumers who aren't seeking coverage for themselves on any eligibility application.
  - Request an individual's SSN if he or she is not seeking coverage for himself or herself, unless the application asks for the individual's income, and it is necessary to determine the applicant's household income.
  - Request information from or concerning any individual who is not seeking coverage for themselves, unless the information is needed for the Marketplace to determine an applicant's eligibility for enrollment in a qualified health plan (QHP) or financial assistance to help pay for health care costs.
  - Collect PII beyond what is necessary to perform your authorized functions without the specific, informed consent of the consumer.
  - Use someone's PII to discriminate against them, such as refusing to assist individuals who are older or have significant or complex health care needs.



Prohibited Requests for Collections or Uses of PII (Cont.)

- 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.

Requirements to Protect PII

Your organization must establish safeguards to ensure that:

- PII is only used by or disclosed to those who are authorized to receive or view it and that have completed Marketplace registration, training, and certification.
- 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 your organization's agreement with CMS or grant terms and conditions, as applicable.
- PII security controls and related system risks are monitored, periodically assessed, and updated to ensure the continued effectiveness of those controls.
- Electronic transmission of PII is conducted through secure electronic interfaces developed and utilized by the organization.

Best Practices to Protect PII: In-Person

- Make sure consumers take possession of their documents.
- Use private spaces when providing application and enrollment assistance.
- Secure hard-copy consumer consent forms in a locked location.
- 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.

Best Practices to Protect PII: Electronic

- 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).
- 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.

Best Practices to Protect PII: Paper

- 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.

Best Practice to Protect PII: Discussion

What are other best practices your organization uses for handling PII, particularly when assisting consumers remotely?

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 privacy breach is a suspected or confirmed incident involving PII. It must pertain to the unauthorized use or disclosure of PII including accidental disclosure such as misdirected e-mails or faxes.
- An incident, or security incident means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
- Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

PII Breaches and Security Incidents (Cont.)

Such policies and procedures must:

- Identify your 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 PII is involved in the incidents. If in doubt, you must reach out to the CMS IT Service Desk at CMS_IT_Service_Desk@cms.hhs.gov.

Reporting a PII Breach or Security Incident

Policies and procedures to handle PII breaches and security incidents must:

- Require all CACs or Navigators to report potential incidents or breaches to the organization.
- Require reporting of any incident or breach to the CMS IT Service Desk (available 24 hours a day, 7 days a week) **within one hour after discovery of the breach or incident**.
  - Phone: 410-786-2580 or 1-800-562-1963
  - Email: CMS_IT_Service_Desk@cms.hhs.gov
- Require the completion of a CMS Security Incident Report.
- Provide details regarding the identification, response, recovery, and follow-up of incidents and breaches.

Reporting a PII Breach or Security Incident (Cont.)

If you have questions about privacy and security requirements, you should direct your questions to:

- Certified Application Counselors: CACQuestions@cms.hhs.gov
- Navigators: NavigatorGrants@cms.hhs.gov
- Enrollment Assistance Personnel: EAPQuestions@cms.hhs.gov

Examples: PII Breaches and Security Incidents

Examples of issues you must report include:

- Lost, stolen, or misplaced records (such as paper files) containing PII.
- Lost, stolen, misplaced, or otherwise compromised electronic records (such as email or other software systems) containing PII.
- Unauthorized personnel seeing or possessing PII.
- Lost, stolen, or misplaced electronic devices (e.g., tablets, phones, or laptops) that contain consumer PII.

Available Resources

- Guidance and regulations on assister programs: CMS.gov/marketplace/in-person-assisters/technical-resources/guidance-regulations.
- Requirements and Best Practices for Assisters on Providing Remote Consumer Assistance: CMS.gov/marketplace/technical-assistance-resources/providing-remote-consumer-assistance.pdf.
- Please also refer, 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.