



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



October 7, 2020

The information provided in this document is intended only to be a general informal summary of technical legal standards. It is not intended to take the place of the statutes, regulations, or formal policy guidance that it is based upon. This document summarizes current policy and operations as of the date it was presented. We encourage readers to refer to the applicable statutes, regulations, and other interpretive materials for complete and current information. This communication was produced and disseminated at U.S. taxpayer expense. The contents of this document do not have the force and effect of law and are not meant to bind the public in any way, unless specifically incorporated into a contract. This document is intended only to provide clarity to the public regarding existing requirements under the law.

Agenda

- Background on FFM (a.k.a., Federally-facilitated Exchange (FFE) or, for purposes of this presentation, Marketplace) Navigator and certified application counselor (CAC) privacy and security requirements and highlights
- How to obtain a consumer's authorization before gaining access to personally identifiable information (PII)
- CAC and Navigator model authorization forms
- Best practices for handling PII
- Additional resources



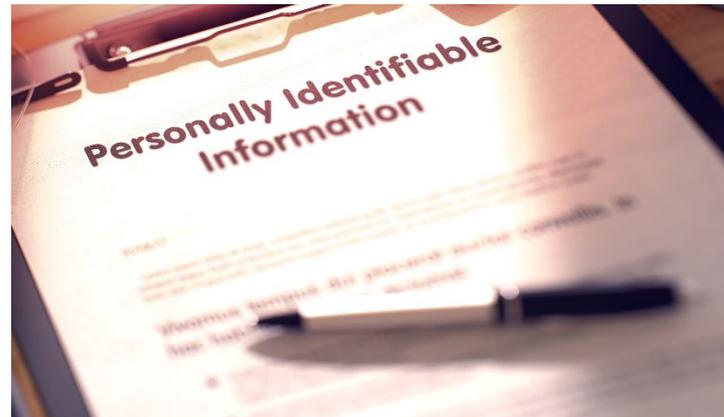
Background on Assister Privacy and Security Requirements

- Navigators and CACs are collectively referred to as assisters throughout this presentation.
- Each assister organization should refer to the privacy and security standards that apply to them.
 - Navigators: Attachments H, I, and J of the 2019-2021 Grant Terms and Conditions.
 - CACs: Formal agreement between CMS and the CAC designated organization (CDO).



What is PII?

- Personally identifiable information (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.
- Examples of PII assisters may collect, disclose, access, maintain, store, and/or use when helping consumers in the Marketplace (Note: This list is not exhaustive):
 - Name
 - Phone number
 - Email address
 - Income
 - Birth date
 - Social Security Number (SSN)



Highlights of Assister Privacy and Security Requirements

- 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, including:
 - Their required assister duties, such as helping a consumer apply for Marketplace, Medicaid, or Children's Health Insurance Program (CHIP) coverage, helping a consumer enroll in coverage, and helping consumers with questions related to their coverage.
 - For other purposes for which the consumer provides his or her specific, written, informed consent.

Highlights of Assister Privacy and Security Requirements (Cont.)

- The assister privacy and security requirements address how these assisters must handle PII. These privacy and security requirements generally are designed to ensure that:
 - Information is used only as is necessary and relevant to perform authorized Marketplace functions or for other purposes for which the consumer provides his or her specific, written, informed consent;
 - All use of consumer PII must have their prior written consent, which can be revoked at any time;
 - Appropriate, swift action is taken when a PII incident or breach occurs; and
 - Confidentiality is protected to enable trust between the assister and the consumer.

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 this privacy notice statement).



What a Privacy Notice Statement Needs to Include

- At a minimum, the *privacy notice statement* must include the following:
 - 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; and
 - What, if any, notice or opportunity for consent will be provided regarding the collection, use, or disclosure of the information.

What a Privacy Notice Statement Needs to Include (Cont.)

- At a minimum, the **privacy notice statement** must include the following:
 - 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; and
 - 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.



How to Obtain a Consumer's Authorization Before Gaining Access to PII

- Detailed resource that provides additional information for assisters in the FFM: [Marketplace.cms.gov/technical-assistance-resources/obtain-consumer-authorization.pdf](https://marketplace.cms.gov/technical-assistance-resources/obtain-consumer-authorization.pdf)
- Assisters are required to:
 - Ensure that consumers are informed of the functions and responsibilities of the assister prior to receiving assistance;
 - Ensure that consumers provide authorization via completing and signing a written form prior to an assister obtaining access to a consumer's PII and that consumers 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.

What a Consumer's Authorization Needs to Include

- At a minimum, a consumer's authorization should include the following:
 - An acknowledgement that you (assister) informed the consumer of the functions and responsibilities that apply to your specific assister role (e.g., Navigator, CAC);
 - Consent for you to access and use the consumer's PII to carry out your Marketplace functions and responsibilities; and
 - An acknowledgement that the consumer may revoke any part of the authorization at any time as well as a description of any limitations that the consumer wants to place on your access to or use of the consumer's PII.



Maintaining a Record of Authorization

- At a minimum, the *record of the authorization* should 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 acknowledgements and consents obtained from the consumer.
 - If any changes are later made to the authorization, include if and when a consumer revoked the authorization or any part thereof.

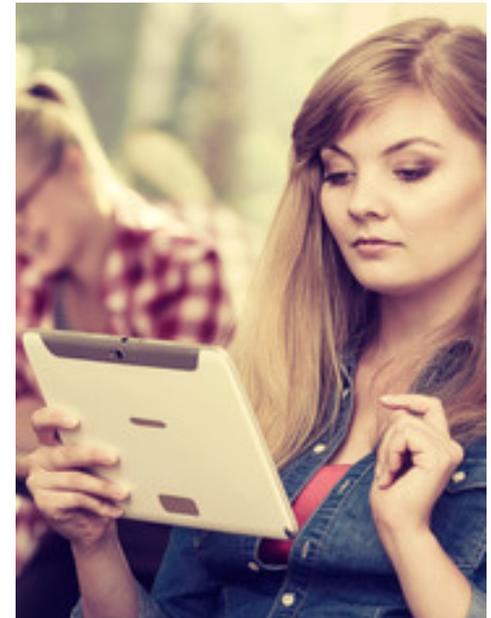
Scenario 1: Assisting a Homebound Consumer Over the Telephone or Computer

- You are assisting a consumer for the first time. Due to the COVID-19 pandemic, you are assisting the consumer remotely over the phone or computer.
- 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 of the authorization that are 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.



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.
- Authorization:
 - You may use a sign-up sheet to collect a consumer's name and contact information as long as you make it clear to the consumer on the face of the sign-up sheet (and orally, if appropriate) that by providing their name and contact information, they are consenting to be contacted for application and enrollment assistance.
 - Any PII collected on the sign-up sheet such as a consumer's name and contact information 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 would need to be retained in accordance with the record requirements stated earlier.
 - 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."



Scenario 3: Consumer Makes Initial Contact and Shares PII

- You and 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.
- Authorization:
 - If a consumer directly contacts you and your organization for assistance and provides his or her 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, and access to it should be given to staff who need to access it to carry out required duties.



Scenario 4: 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 his or her PII with you.
- Authorization:
 - Generally speaking, you are permitted to follow up with the consumer so long as the third party who contacts you confirms that she has obtained the consumer's consent to share her 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.



CAC and Navigator Model Authorization Forms

- CAC model authorization in [English](#) and [Spanish](#).

Updated 2017¹

Model Authorization Form for Certified Application Counselors (CACs) in a Federally-facilitated Marketplace¹ (Marketplace)

CAC Designated Organization Name: _____

CAC Designated Organization Address: _____

CAC Designated Organization Phone Number and Email: _____

Individual CAC Name and Certification Number: _____

I. Acknowledgement of Roles and Responsibilities of CACs (see Attachment A)

I have been informed about and understand the CAC roles and responsibilities set forth on Attachment A and have been given the opportunity to discuss them with [Name].²

II. Definitions and Explanations of Terms Used in This Form

In this authorization form:

- The words "I," "me," or "my" include my authorized representative if I have one.
- Personally identifiable information is called "PII." Examples of my PII include, but are not limited to my name, phone number, email address, home address, immigration status, income, and household size information.
- Health plans available through the Marketplace are called Qualified Health Plans or "QHPs."
- Other programs called "insurance affordability programs" are also available through the Marketplace. These programs can help me or my family pay for health coverage, and include public programs, such as Medicaid or the Children's Health Insurance Program (CHIP), premium tax credits, cost-sharing reductions, and, if one is available in my state, the Basic Health Program.

III. Authorizations

a. General Consent

I, _____, give my permission to [Name], including the individual CACs who are certified by this CAC designated organization, to create, collect, disclose, access, maintain, store, and/or use my PII in order to carry out the roles and responsibilities of a CAC that are authorized by federal regulation and generally summarized in Attachment A, unless I have limited that consent as set forth in _____

¹ Including Federally-facilitated Marketplaces where the state performs plan management functions.
² NOTE TO CAC DESIGNATED ORGANIZATION AND INDIVIDUAL CAC: Each time [Name] appears in this Authorization Form, the Name of the CAC Designated Organization, at a minimum, should be inserted. Individual CAC name(s) may, but are not required, to be inserted.

- Navigator model authorization in [English](#) and [Spanish](#).

Updated 2017¹

Model Authorization Form for Navigators in a Federally-facilitated Marketplace¹ (Marketplace)

Navigator Organization Name: _____

Navigator Organization Address: _____

Navigator Organization Phone Number and Email Address: _____

Individual Navigator Name or Staff/Volunteer Name and Certification Number: _____

I. Acknowledgement of Roles and Responsibilities of Navigators (see Attachment A)

I have been informed about and understand the Navigator roles and responsibilities set forth on Attachment A and have been given the opportunity to discuss them with [Name].²

II. Definitions and Explanations of Terms Used in This Form

In this authorization form:

- The words "I," "me," or "my" include my authorized representative if I have one.
- Personally identifiable information is called "PII." Examples of my PII include, but are not limited to my name, phone number, email address, home address, immigration status, income, and household size information.
- Health plans available through the Marketplace are called Qualified Health Plans or "QHPs."
- Other programs called "insurance affordability programs" are also available through the Marketplace. These programs can help me or my family pay for health coverage, and include public programs, such as Medicaid or the Children's Health Insurance Program (CHIP), premium tax credits, cost-sharing reductions, and, if one is available in my state, the Basic Health Program.

III. Authorizations

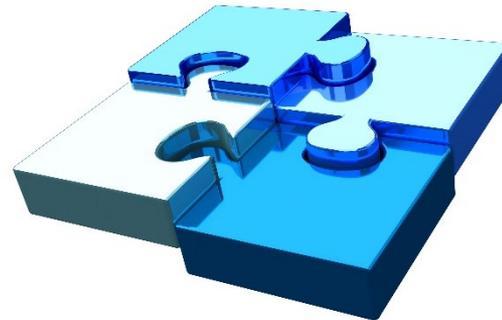
a. General Consent

I, _____, give my permission to [Name], including the individual Navigators who are a part of this Navigator organization, to create, collect, disclose, access, maintain, store, and/or use my PII in order to carry out the roles and responsibilities of a Navigator that are authorized by federal statute and regulation and generally summarized in Attachment A, unless I have limited that consent as set forth in this document. I understand that [Name] might need to create, collect, disclose, access, maintain, store, and/or use some of my _____

¹ Including Federally-facilitated Marketplaces where the state performs plan management functions.
² NOTE TO NAVIGATOR ORGANIZATION AND INDIVIDUAL NAVIGATOR: Each time [Name] appears in this Authorization Form, the Name of the Navigator Organization, at a minimum, should be inserted. Individual Navigator name(s) may, but are not required, to be inserted.

CAC and Navigator Model Authorization Forms (Cont.)

- Four main parts:
 1. Acknowledgement that 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.
 2. Definition of terms.
 3. Authorizations:
 - General consent.
 - Specific consent(s).
 - Exceptions or limitations to consents .
 - Additional information about the Navigator’s or CAC’s use of consumer PII.
 4. Signature and space for consumer to provide contact information for follow-up.



CAC 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 the consumer provides his or her contact information.
 - Might share the consumer's PII if referring consumers to another source of help.
 - Should provide the consumer with copies of the completed authorization form and the Navigator's or CAC's roles and responsibilities in Attachment A.

Requirements and Best Practices for Handling PII

- More detailed information for Navigators and CACs in the FFM:

[Marketplace.cms.gov/technical-assistance-resources/assister-programs/best-practices-for-handling-pii-fast-facts.pdf](https://marketplace.cms.gov/technical-assistance-resources/assister-programs/best-practices-for-handling-pii-fast-facts.pdf)

Requirements and Best Practices for Assisters on Handling Personally Identifiable Information

Updated 2017

This Fact Sheet Applies If You:

- Are a Navigator or certified application counselor (collectively, an assister) in a state with a Federally-facilitated Marketplace¹
- Have questions about personally identifiable information (PII)
- Are looking for best practices and tips on handling PII

Personally Identifiable Information (PII): Overview

As a Navigator or certified application counselor (CAC) (collectively referred to as an "assister") helping consumers who are applying for health insurance through a Federally-facilitated Marketplace, you may encounter consumers' personally identifiable information (PII). This document contains suggested measures to take for protecting consumers' personally identifiable information (PII) in the course of performing assister duties.

PII is anything that could individually, or in combination with other data elements, identify the consumer, such as a consumer's name, address, telephone number, social security number, Marketplace application ID or other identifier.² Consumers must have an opportunity to access, inspect, and/or correct their PII if they make a request to do so. 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, including their required assister

¹ The terms "Federally-facilitated Marketplace" and "FFM," as used in this document, include FFM where the state performs plan management functions and State Partnership Marketplaces.

² According to the privacy and security standards set forth in Navigators' grant terms and conditions, certified application counselor organizations' agreements with CMS, PII is defined as "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. (OMB Memorandum M-17-12 [January 3, 2017])."

Requirements and Best Practices for Handling PII (Cont.)

- Prohibitions on accessing and using 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.
 - Don't 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.
 - 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.

***Note:** 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 and Best Practices for Handling PII (Cont.)



- 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 securely destroyed and 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 systems 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 for Handling PII

- Use private spaces when providing application and enrollment assistance.
- Don't leave files or documents containing PII or tax return information unsecured and unattended.
- Don't send or forward emails with PII to personal email accounts.
- Protect emails that contain PII (e.g., encryption).
- Lock up portable devices (e.g., laptops, cell phones).

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

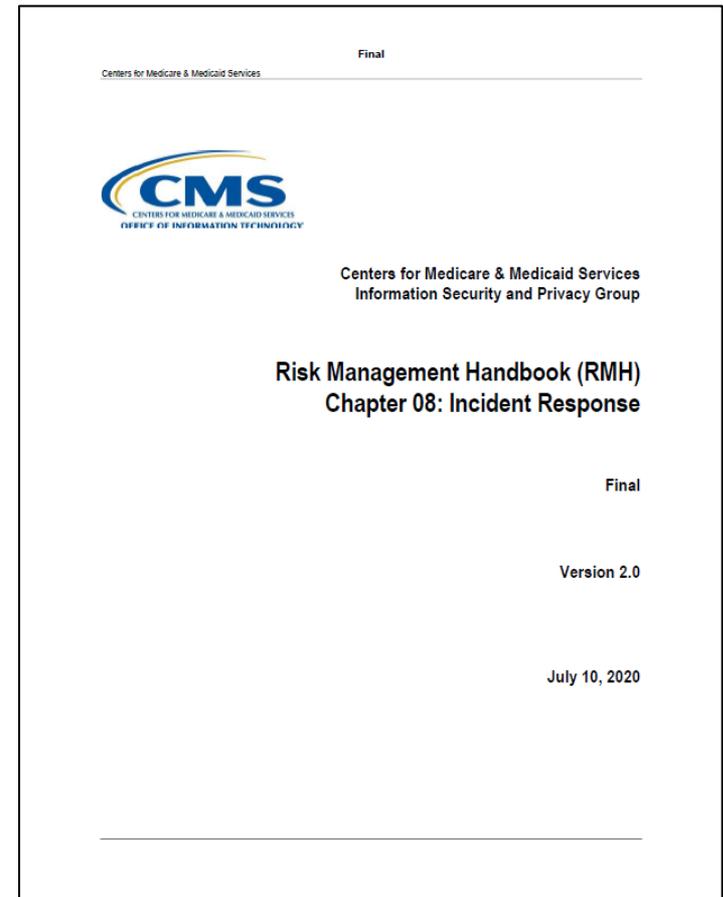
Best Practices for Handling PII (Cont.)

- Clear your web browser history to avoid other users accessing PII.
- 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.
- 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.



Requirements for Handling PII (Cont.)

- **Reporting PII Breaches:** Assister organizations must implement and comply with policies and procedures to handle PII breaches and security incidents consistent with [CMS' Risk Management Handbook Standard 7.1 Incident Handling and Breach Notification](#).
- 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.



Requirements for Handling PII (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.



Requirements for Handling PII (Cont.)

- Such policies and procedures 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 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.
 - Require the completion of a CMS Security Incident Report.
 - Provide details regarding the identification, response, recovery, and follow-up of incidents and breaches.

Requirements for Handling PII (Cont.)

- Examples of issues you should 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.



Who to Contact for Questions and Reporting Breaches

- 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
 - Reporting incidents or breaches: Contact 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](mailto:CMS_IT_Service_Desk@cms.hhs.gov)



Available Resources

- Guidance: [How to obtain a consumer's authorization before gaining access to personally identifiable information \(PII\).](#)
- Guidance: [Requirements and best practices for assisters on handling personally identifiable information \(PII\).](#)
- Model Authorization Form for Navigators in a FFM in [English](#) and [Spanish](#).
- Model Authorization Form for CACs in a FFM in [English](#) and [Spanish](#).