CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

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

Center for Consumer Information and Insurance Oversight

February 2016

A Note about this Presentation

- The information provided in this presentation 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, grant terms & conditions, agreements, and formal policy guidance that it is based upon. This presentation summarizes current policy and operations as of the date it was presented.
- Links to certain source documents have been provided for your reference. We encourage audience members to refer to the applicable statutes, regulations, grant terms & conditions, agreements, and other interpretive materials for complete and current information.

Agenda

1. Background on FFM Navigator and certified application counselor (CAC) privacy and security requirements and highlights
2. How to obtain a consumer's authorization before gaining access to PII
3. CAC and Navigator model authorization forms
4. Best practices for handling PII
5. What additional resources are available?

3

1. Background on FFM Navigator and CAC Privacy and Security Requirements

- All Marketplaces are required to have privacy and security standards. **The Federally-facilitated Marketplace (FFM) establishes FFM Navigator and CAC privacy and security standards through grant terms and conditions and agreements.**
- Each FFM Navigator and CAC organization should refer to the privacy and security standards that apply to them. These are included in the following:
  - **Navigators:** Attachments E and F of grant terms and conditions
  - **CACs:** Agreement between CMS and CAC designated organization

4

What is "PII"?

- **Personally Identifiable Information (PII)** includes any information that:
  - can be used to distinguish or trace an individual's **identity**,
  - alone or when **combined** with other personal or identifying information
  - that is **linked** or **linkable** to that individual

OMB Memorandum M-07-16

Examples: name, social security number, biometric records, date and place of birth, mother's maiden name, etc.

CMS

5

Highlights of FFM Navigator and CAC Privacy and Security Requirements

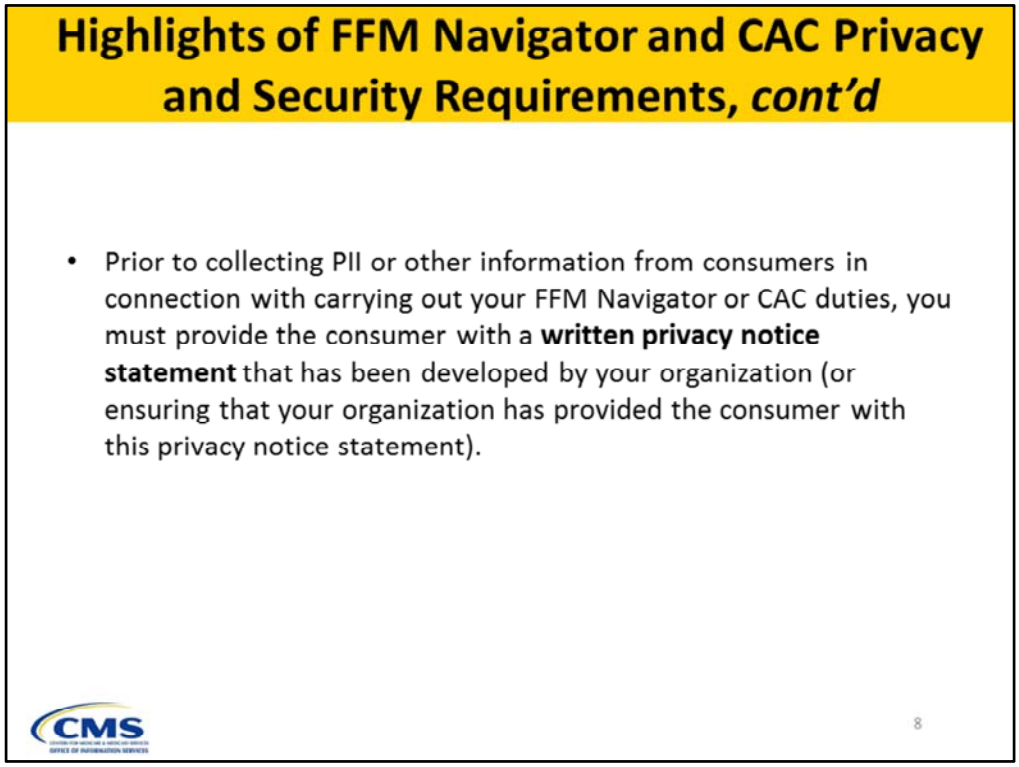
- FFM Navigators and CACs **are permitted to create, collect, disclose, access, maintain, store and use consumer PII only** to perform functions that they are authorized to perform as assisters, including:
  - Their required assister duties
  - Or for other purposes for which the consumer provides his or her specific, informed consent.

6

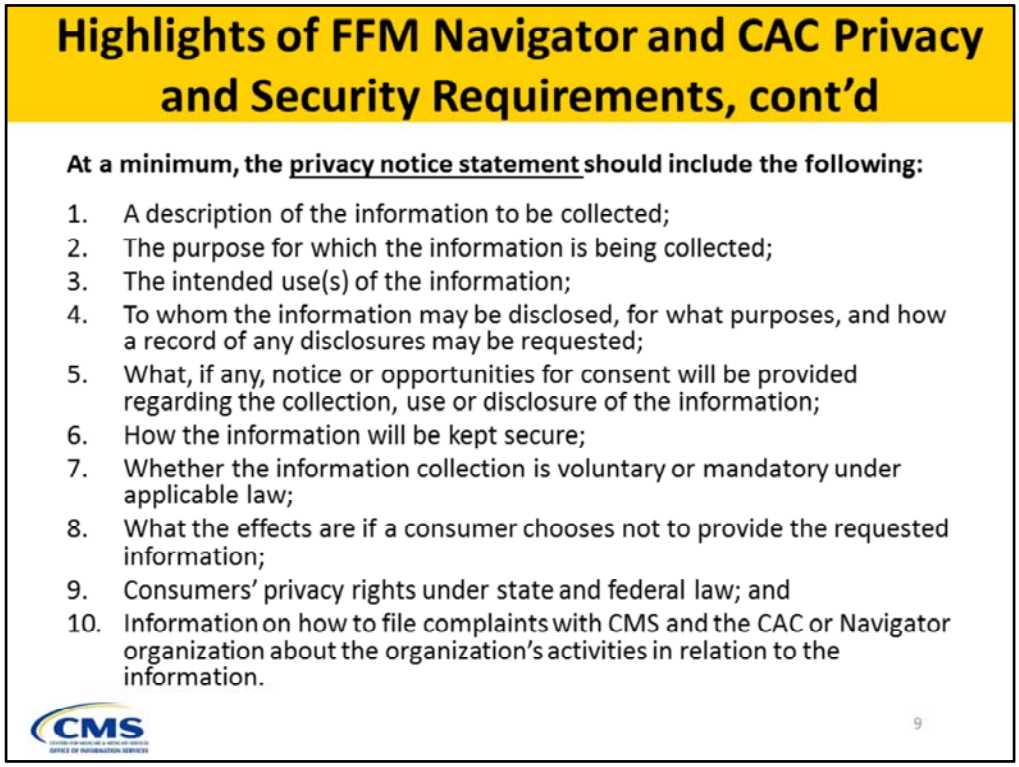
Highlights of FFM Navigator and CAC Privacy and Security Requirements, *cont'd*

- The FFM Navigator and CAC privacy and security requirements address how these assisters should 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 functions, or for other purposes for which the consumer provides his or her specific, informed consent;
  - All uses of their PII are consented to by the consumer;
  - Appropriate, swift action is taken when an incident or breach occurs; and
  - Confidentiality is protected, to enable trust between the assister and the consumer.

7



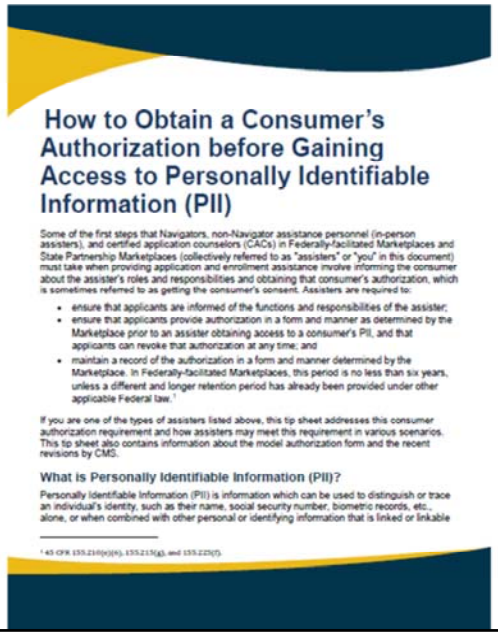
However, the privacy notice statement doesn't need to be provided to consumers prior to collecting their name, physical address, email address or telephone number if that information is being used solely for making future contact with the consumer to carry out an authorized function, such as setting up an appointment, or to send them educational information directly related to your authorized functions.



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 living with disabilities and with limited English proficiency.

Assister organizations must review their privacy notice statement and revise it as necessary on an annual basis, at a minimum, and before or as soon as possible after any change to its privacy policies and procedures.

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



How to Obtain a Consumer's Authorization before Gaining Access to Personally Identifiable Information (PII)

Some of the first steps that Navigators, non-Navigator assistance personnel (in-person assisters), and certified application counselors (CACs) in Federally-facilitated Marketplaces and State Partnership Marketplaces (collectively referred to as "assisters" or "you" in this document) must take when providing application and enrollment assistance involve informing the consumer about the assister's roles and responsibilities and obtaining that consumer's authorization, which is sometimes referred to as getting the consumer's consent. Assisters are required to:

- ensure that applicants are informed of the functions and responsibilities of the assister;
- ensure that applicants provide authorization in a form and manner as determined by the Marketplace prior to an assister obtaining access to a consumer's PII, and that applicants can revoke that authorization at any time; and
- maintain a record of the authorization in a form and manner determined by the Marketplace. In Federally-facilitated Marketplaces, this period is no less than six years, unless a different and longer retention period has already been provided under other applicable Federal law.[1]

If you are one of the types of assisters listed above, this tip sheet addresses this consumer authorization requirement and how assisters may meet this requirement in various scenarios. This tip sheet also contains information about the model authorization form and the recent revisions by CMS.

What is Personally Identifiable Information (PII)?

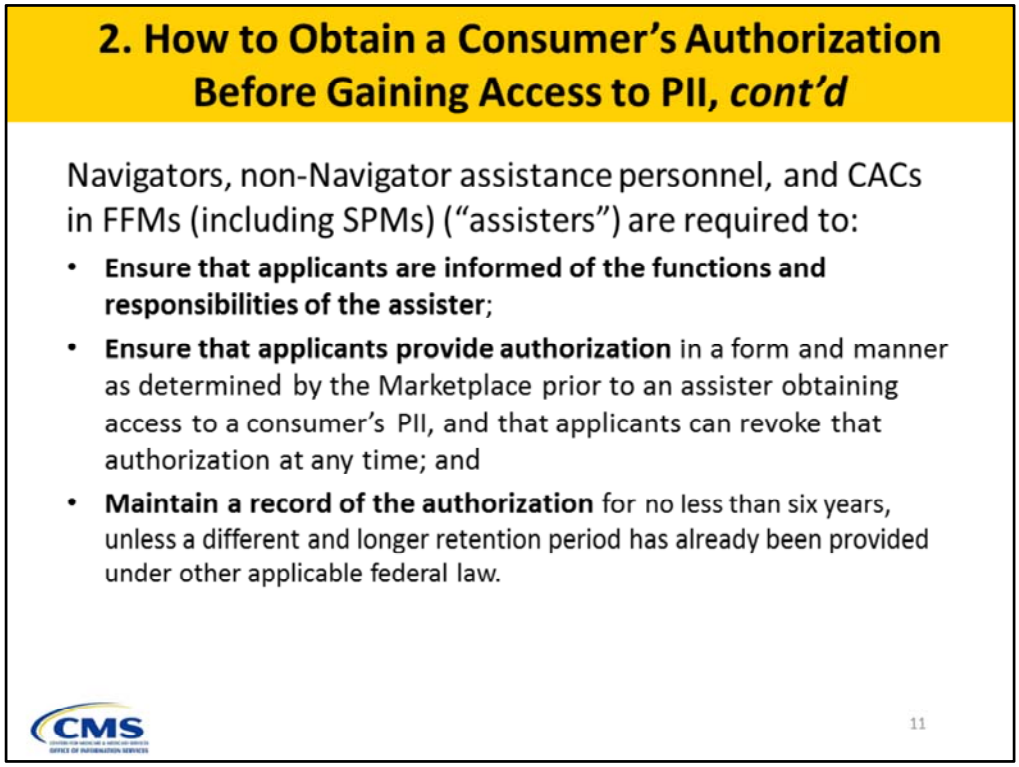
Personally Identifiable Information (PII) is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable

[1] 45 CFR 155.210(e)(8), 155.215(g), and 155.225(f).

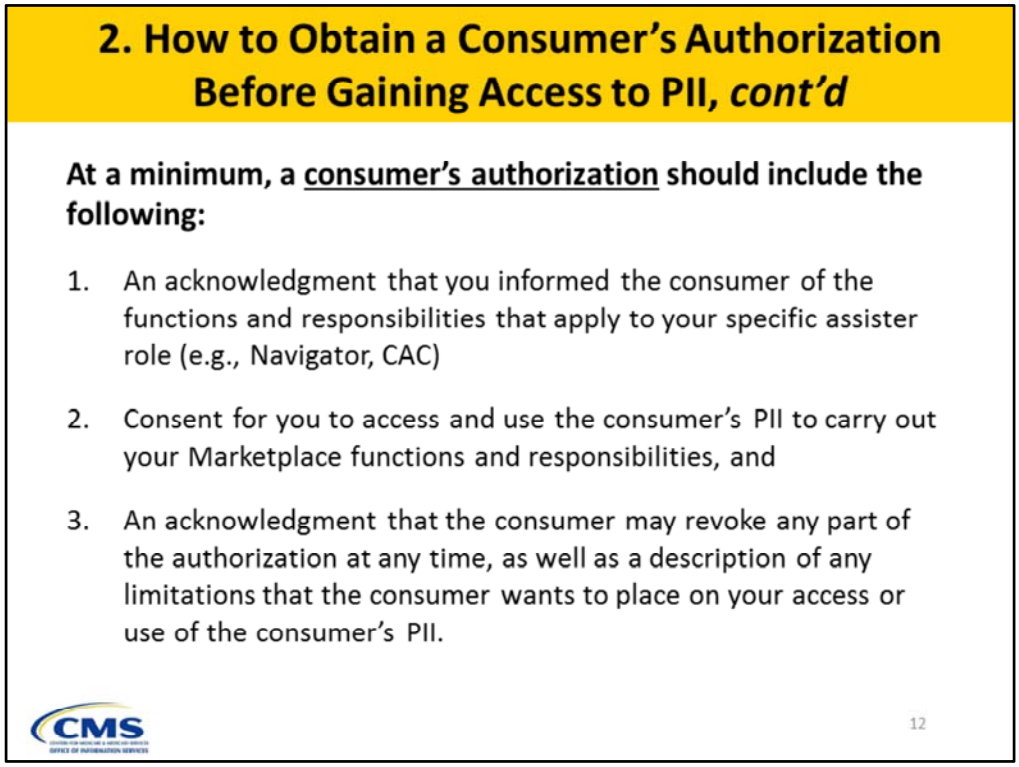
https://marketplace.cms.gov/technical-assistance-resources/obtain-consumer-authorization.pdf

Generally applies to Navigators, non-Navigator assistance personnel, and CACs in FFMs (including State Partnership Marketplaces) ("assisters")

10

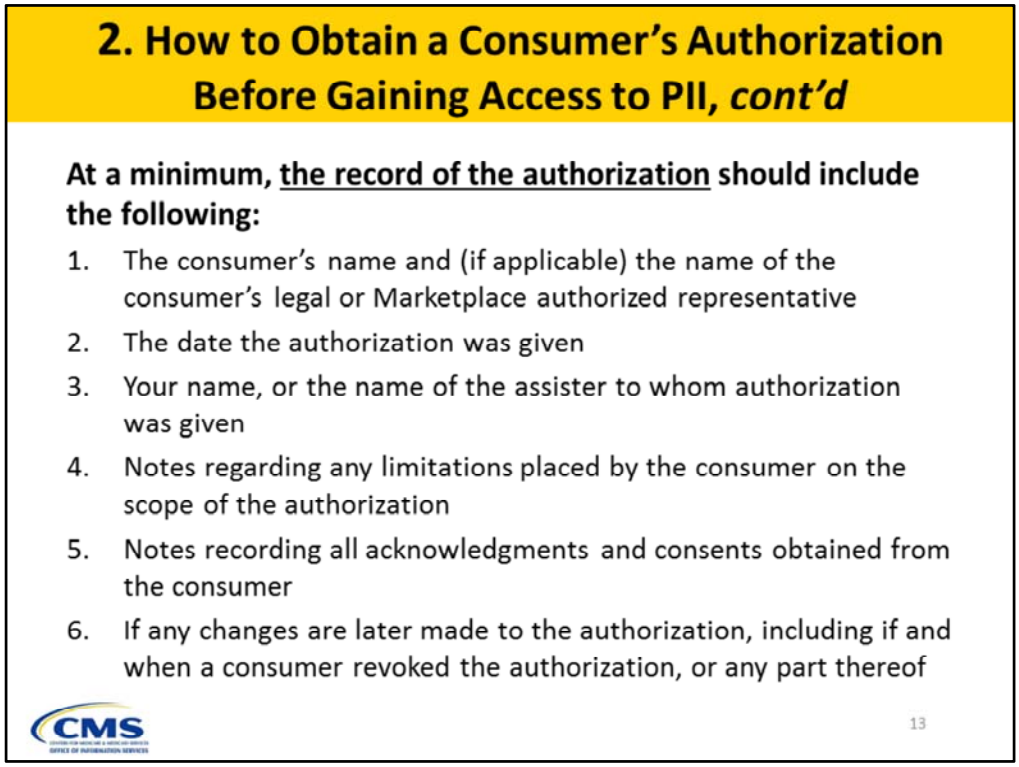


There is a model authorization form that Navigators and CACs in FFM states can use and adapt.



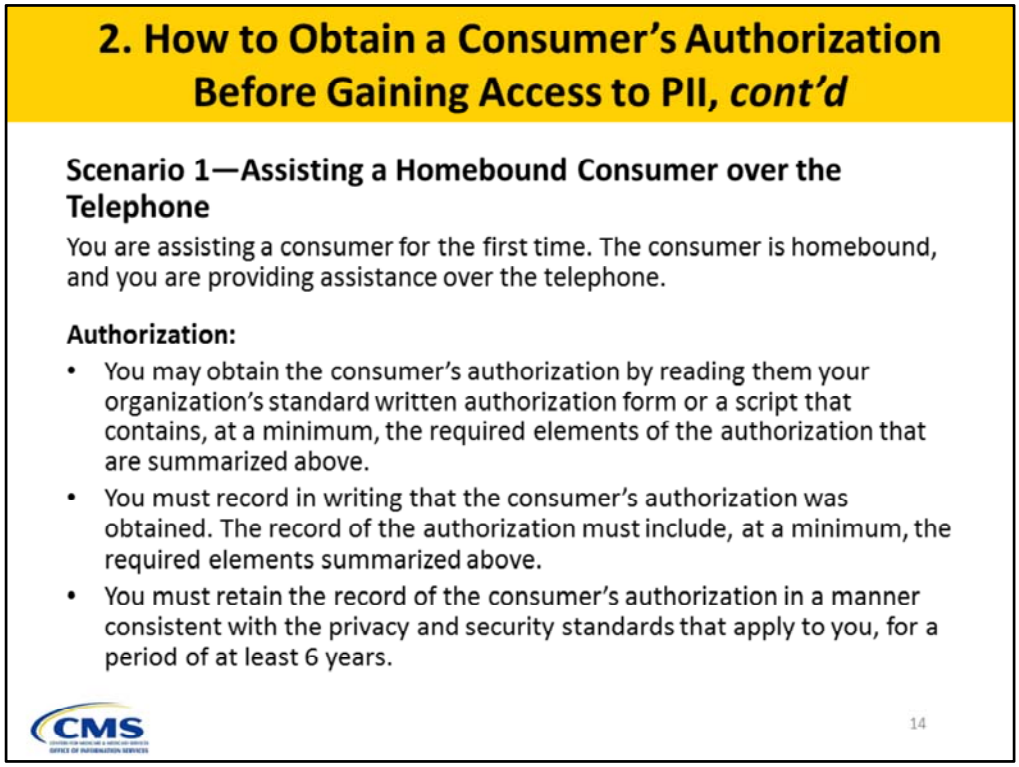
At a minimum, a consumer's authorization should include the following:

1. An acknowledgment that you informed the consumer of the functions and responsibilities that apply to your specific assister role (e.g., Navigator, CAC) (including all the consumer protection standards that apply through CMS regulations to your assister type, such as conflict of interest requirements, rules about accepting payment and providing gifts, etc.);
2. Consent for you to access and use the consumer's PII to carry out your Marketplace functions and responsibilities; and
3. An acknowledgment 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 or use of the consumer's PII.



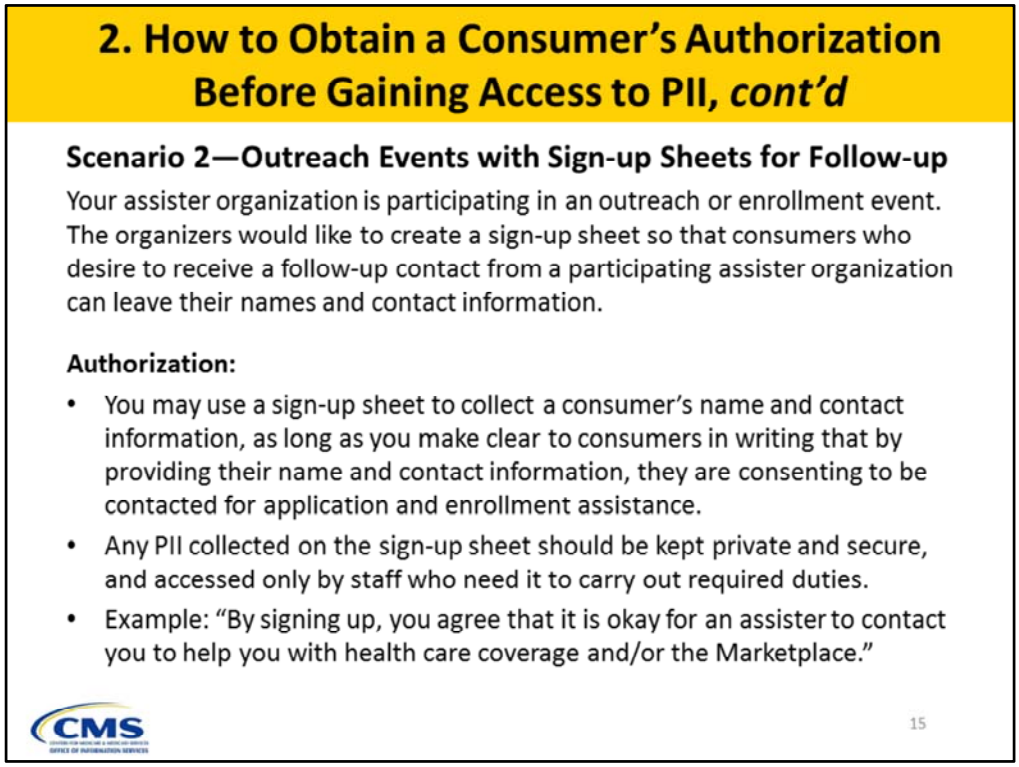
At a minimum, <u>the record of the authorization</u> should include the following:

1. The consumer's name and (if applicable) the name of the legal or Marketplace authorized representative who provides authorization on the consumer's behalf;
2. The date the authorization was given;
3. Your name, or the name of the assister to whom authorization was given. Note that this could include additional names of assisters if the consumer authorized multiple assisters within the same assister organization to obtain access to his or her PII;
4. Notes regarding any limitations placed by the consumer on the scope of the authorization;
5. Notes recording all acknowledgments and consents obtained from the consumer, including any applicable specific consents to access consumer PII for CMS-approved purposes that are not already captured in the list of purposes set forth in your agreement with CMS; and
6. If any changes are later made to the authorization, including if and when a consumer revoked the authorization, or any part thereof, this should be included with the original record.



Be sure to make special notations documenting all consents provided by the consumer and any limitations placed by the consumer on their consents.

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 recommend that you provide a copy of the record to the consumer at the earliest available opportunity.



- Unless this authorization contains the minimum elements summarized above, it does not meet the regulatory requirements, and should be followed up with a more complete authorization if and when you follow up with the consumer.
- Even if this authorization does include all the required minimum elements, we strongly encourage you to obtain the consumer's authorization again when you follow up with them, following your organization's standard authorization procedures.
- FFM Navigators and CACs do not need to provide a privacy notice statement to consumers who provide their name and contact information on such a sign-up sheet.

2. How to Obtain a Consumer's Authorization Before Gaining Access to PII, *cont'd*

Scenario 3—Consumer makes initial contact and shares PII

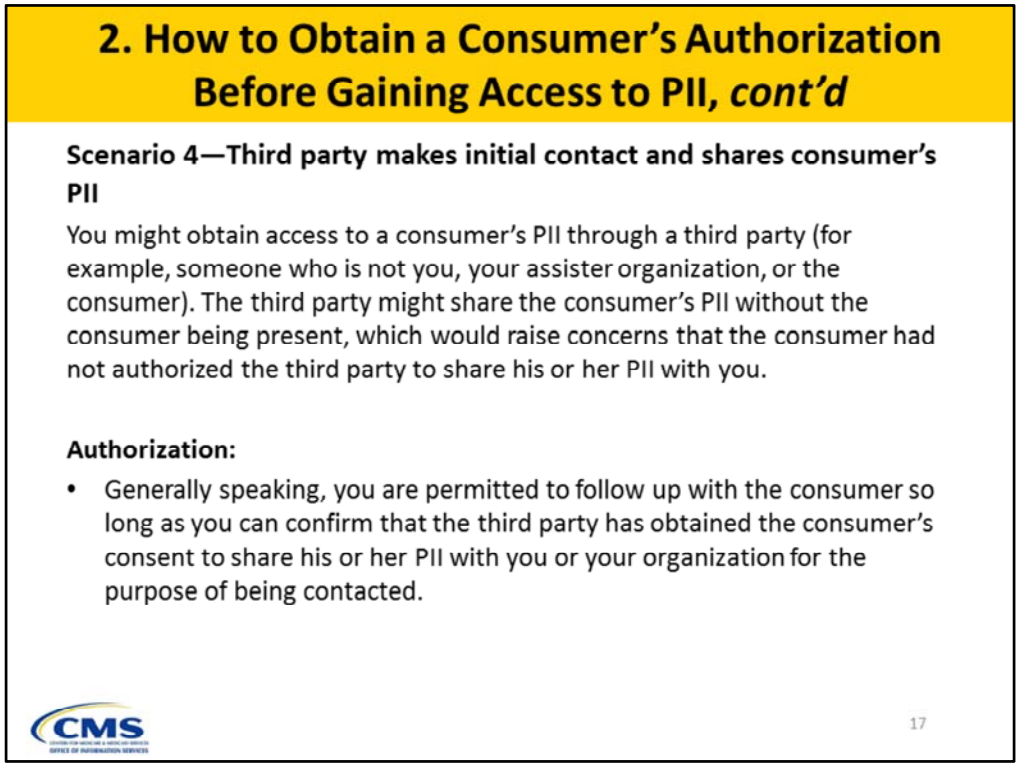
You or your assister organization may receive a direct phone call, voicemail, or email from a consumer requesting your services as an assister. This communication will likely disclose the consumer's PII.

Authorization:

- If a consumer directly contacts you or your organization, the consumer is providing his or her implicit authorization for you or your organization to obtain access to the PII shared with you during the contact.
- Any PII collected during or by means of the initial contact should be kept private and secure, and accessed only by staff who need it to carry out required duties.
- This implicit authorization most likely does not contain all the elements listed above as minimum required elements for the authorization, so you must obtain a complete authorization from the consumer either during the first contact, or the next time you follow up with or meet in-person with the consumer.

CMS

16



Examples of scenarios in which this type of consumer consent may occur are the following:

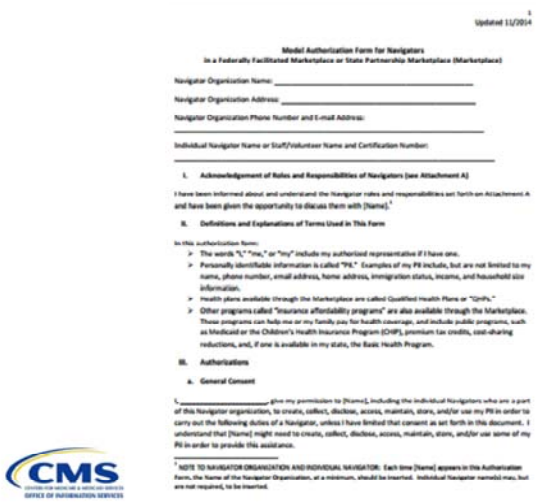
- A third party operates a phone bank event, informs the consumer about the availability of application and enrollment assistance in the area, and obtains the consumer's consent over the phone to share his or her contact information with an assister organization for follow-up. To prove that the third party obtained the consumer's consent, the third party shares documentation of the consumer's consent to a follow-up contact with the assister organization, and the assister organization retains this documentation for its records.
- A third party holds an outreach and education event about the Marketplace. At the event, the third party hands out postcards that consumers may fill out with their contact information to leave with the third party. To document that the third party obtained the consumer's consent, the form language on the postcard clearly indicates that by filling out the postcard, the consumer agrees to be contacted by an assister organization for follow-up. The third party shares these cards with the assister organization, and the assister organization keeps the completed cards on file as documentation that consumer authorization for the follow-up contact has been obtained.

Please note: In any case in which a third party has obtained a consumer's authorization to receive a follow-up contact from an assister, it will nearly always be the case that this preliminary authorization does not contain all the minimum required elements under the rules applicable to Marketplace assisters. Therefore, you must obtain a complete authorization from the consumer when you follow up with the consumer or meet in-person with the consumer, as appropriate. Additionally, any PII collected from the third-party

organization should be maintained privately and securely and access to it should be given only to staff who need to access it to carry out required duties.

3. CAC and Navigator Model Authorization Forms

- CAC model authorization in English and Spanish.
- Navigator model authorization in English and Spanish.



Updated 11/2014

Model Authorization Form for Navigators
in a Federally Facilitated Marketplace or State Partnership Marketplace (Marketplace)

Navigator Organization Name: _____

Navigator Organization Address: _____

Navigator Organization Phone Number and E-mail 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].[1]

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.

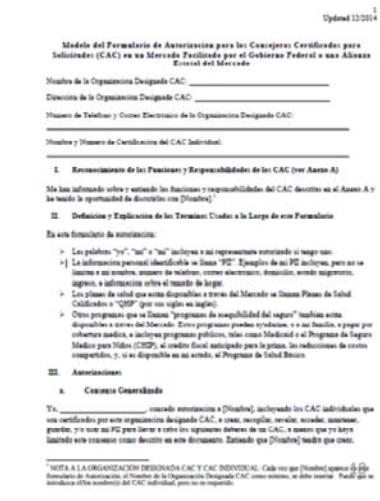
III. Authorizations

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 following duties of a Navigator, 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 PII in order to provide this assistance.

_____

[1] 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.



Updated 12/2014

Modelo del Formulario de Autorización para los Consejeros Certificados para Solicitudes (CAC) en un Mercado Facilitado por el Gobierno Federal o una Alianza Estatal del Mercado

Nombre de la Organización Designada CAC: _____

Dirección de la Organización Designada CAC: _____

Número de Teléfono y Correo Electrónico de la Organización Designada CAC:
_____

Nombre y Número de Certificación del CAC Individual:
_____

I. Reconocimiento de los Funciones y Responsabilidades de los CAC (ver Anexo A)

Me han informado sobre y entiendo las funciones y responsabilidades del CAC descritos en el Anexo A y he tenido la oportunidad de discutirlos con [Nombre].[1]

II. Definición y Explicación de los Terminos Usados a lo Largo de este Formulario

En este formulario de autorización:

- Las palabras "yo", "mi" o "mí" incluyen a mi representante autorizado si tengo uno.
- La información personal identificable se llama "PII". Ejemplos de mi PII incluyen, pero no se limitan a mi nombre, número de teléfono, correo electrónico, domicilio, estado migratorio, ingreso, e información sobre el tamaño de hogar.
- Los planes de salud que están disponibles a través del Mercado se llaman Planes de Salud Calificados o "QHP" (por sus siglas en inglés).
- Otros programas que se llaman "programas de asequibilidad del seguro" también están disponibles a través del Mercado. Estos programas pueden ayudarme, a mí o mi familia, a pagar por cobertura medica, e incluyen programas públicos, tales como Medicaid o el Programa de Seguro Medico para Niños (CHIP), el crédito fiscal anticipado para la prima, las reducciones de costo compartidos, y, si es disponible en mi estado, el Programa de Salud Básico.

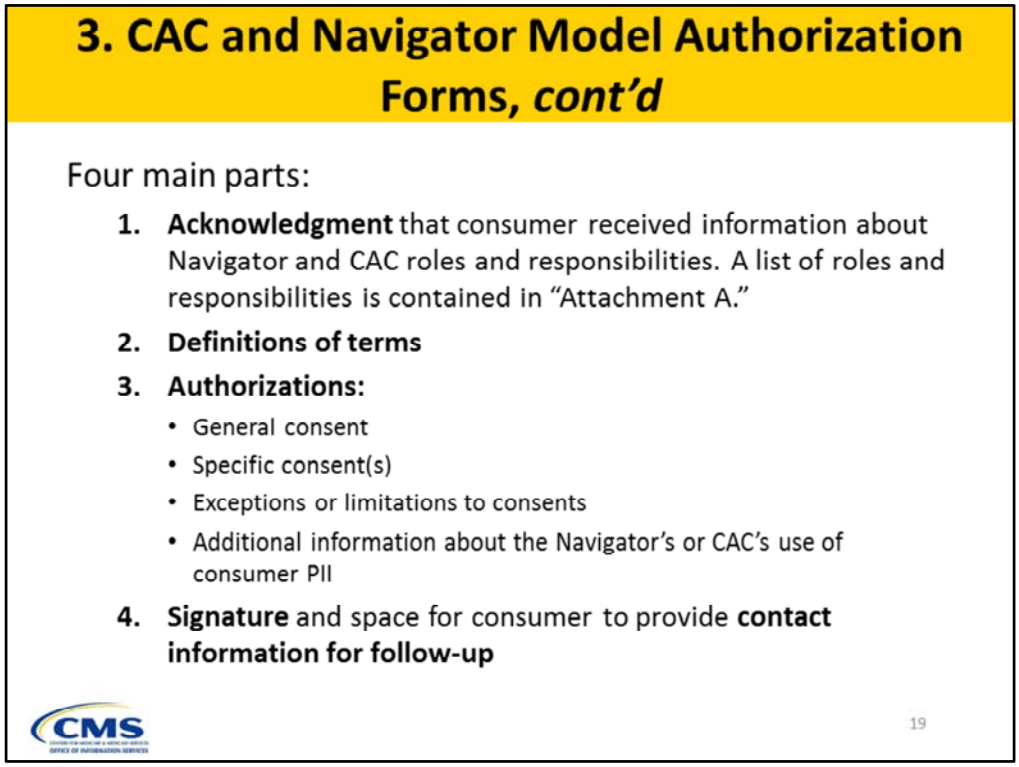
III. Autorizaciones

a. Consenso General

Yo, _____, concedo autorización a [Nombre], incluyendo los CAC individuales que son certificados por esta organización designada CAC, a crear, recopilar, revelar, acceder, mantener, guardar, y/o usar mi PII para llevar a cabo los siguientes deberes de un CAC, a menos que yo haya limitado este consenso como describe en este documento. Entiendo que [Nombre] tendrá que crear,

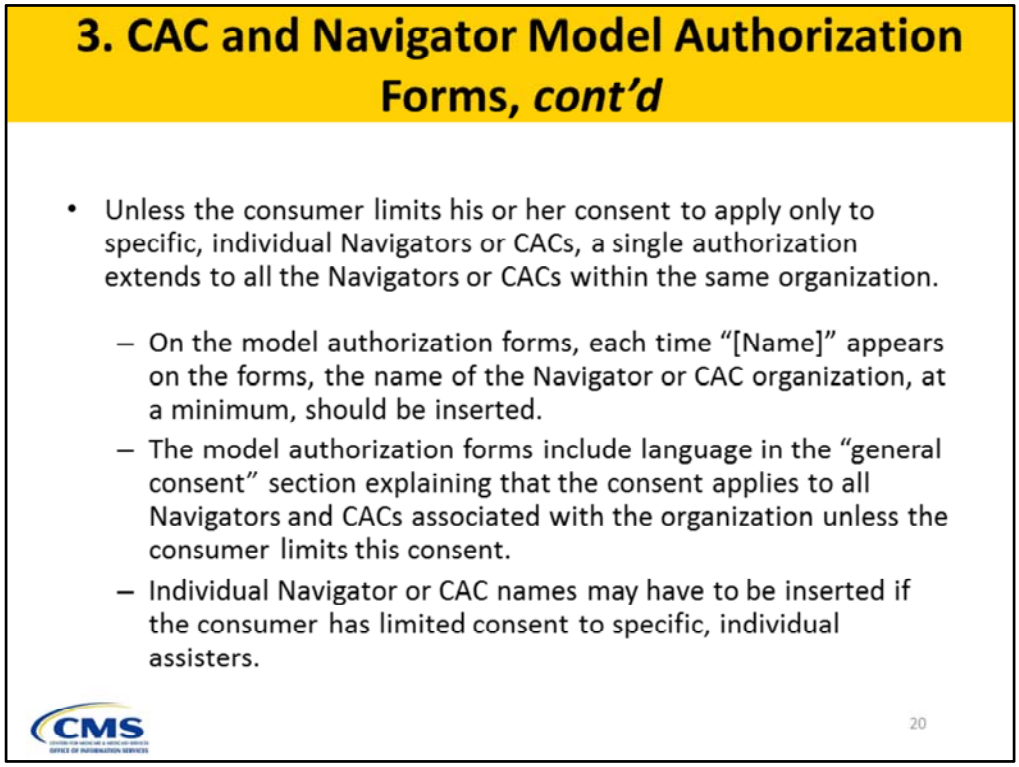
_____

[1] NOTA A LA ORGANIZACIÓN DESIGNADA CAC Y CAC INDIVIDUAL: Cada vez que [Nombre] aparece en este formulario de Autorización, el Nombre de la Organización Designada CAC como mínimo, se debe insertar. Puede que se introduzca el/los nombre(s) del CAC individual, pero no es requerido.

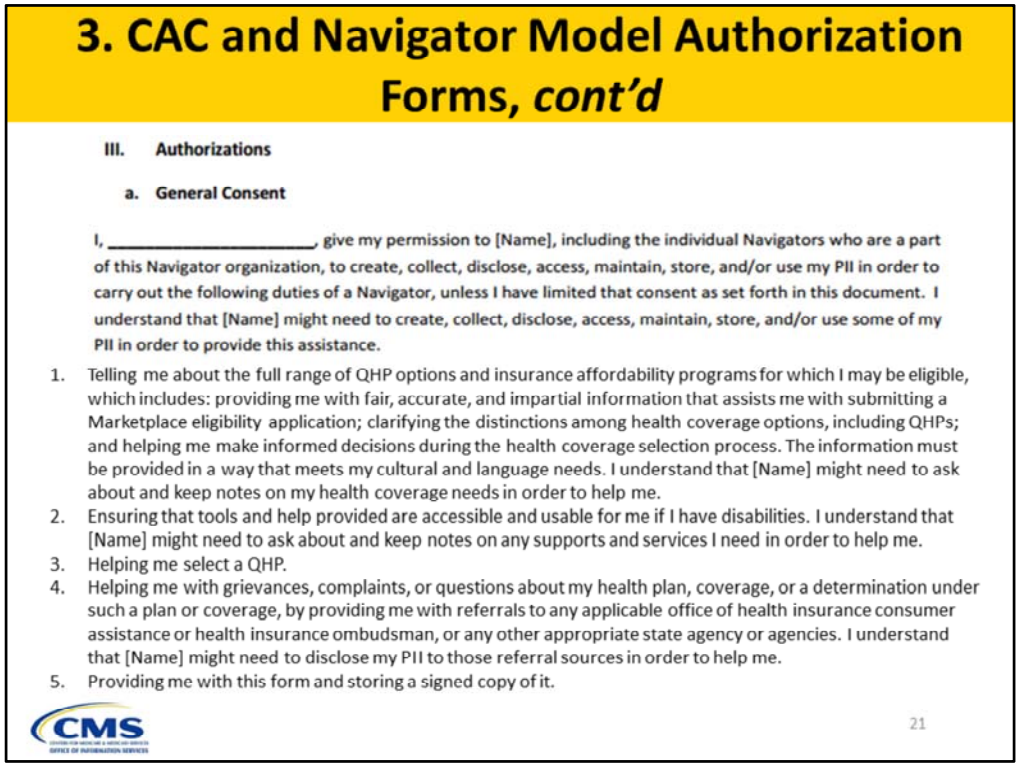


The general consent allows the Navigator or CAC create, collect, disclose, access, maintain, store and use consumer PII to perform functions that they are authorized to perform as Navigators or CACs.

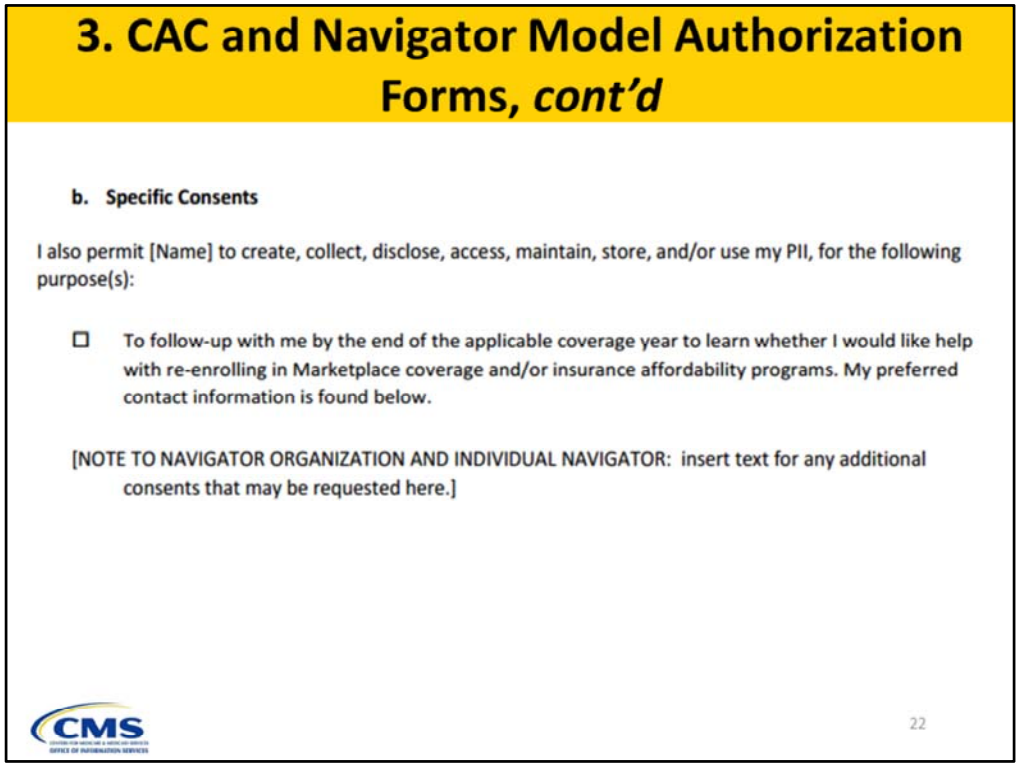
The specific consent(s) allow the Navigator or CAC create, collect, disclose, access, maintain, store and use consumer PII for other specified purposes.



This means that unless the consumer limits his or her consent to apply only to specific individual Navigators or CACs, it is not necessary for a consumer to provide a separate authorization for each individual Navigator or CAC who helps that consumer.



Note that the additional information section specifies that if a consumer gives her contact information when signing this form, her general consent includes permission for the Navigator or CAC to follow up with her about applying for or enrolling into coverage after her first meeting with them.



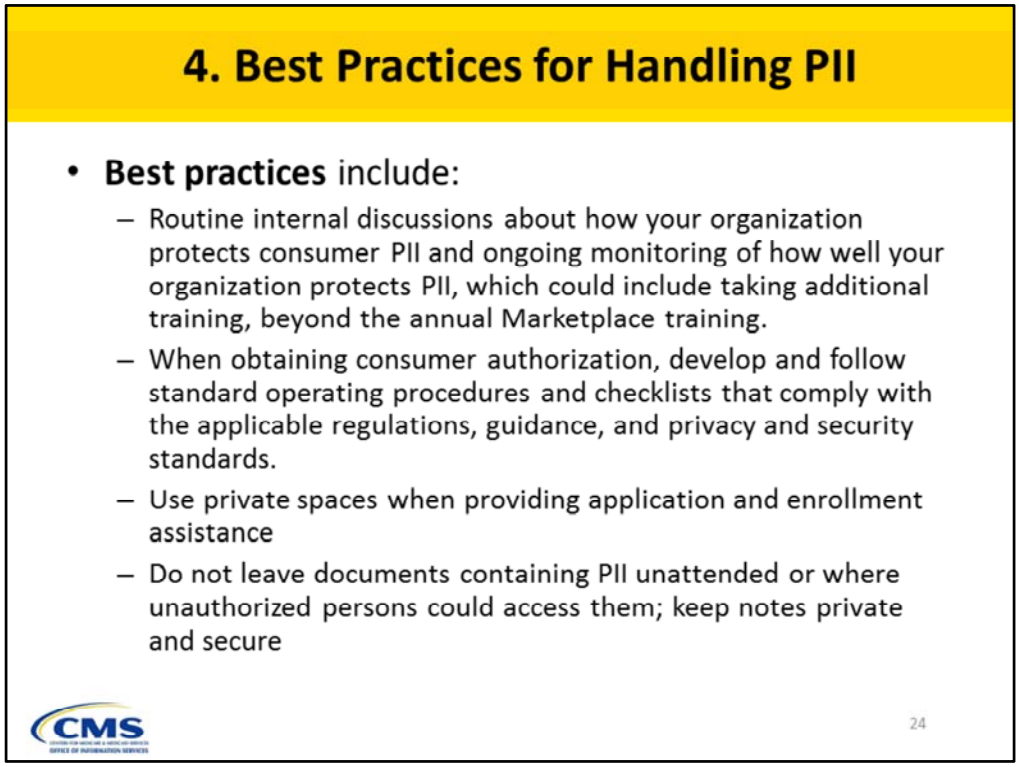
CMS considers that if a consumer already provided his or her consent to an assister to follow up with the consumer on applying for or enrolling in coverage, the assister would be permitted (but not required) to contact the consumer to offer his or her assistance with the annual Marketplace eligibility redetermination and re-enrollment processes. To make it more clear that the consumer's consent would also apply to this activity, we included language providing a specific consent covering this activity in the Navigator and CAC model authorization forms.

Specific authorization can also be added so that consumers can consent to follow-up for additional post-enrollment assistance, if needed. In some cases, post-enrollment assistance might be part of an existing Navigator or CAC duty described as an "authorized function" in Navigator grant terms and conditions and the CAC organization agreements with CMS, and listed on the model authorization forms under the general consent section. Specific consent is not required for uses of consumer PII that fall within the scope of one of these authorized functions. In other cases, consumers should be asked to provide specific consent.

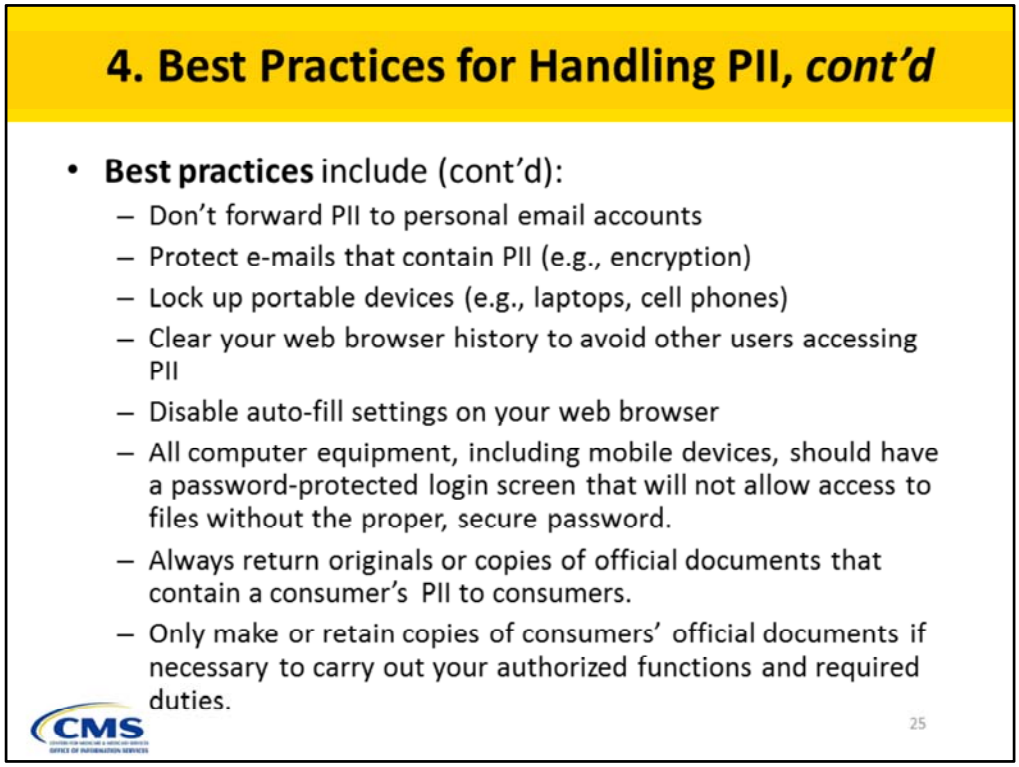
3. CAC and Navigator Model Authorization Forms, *cont'd*

- The **additional information** section, among other things, specifies that the Navigator or CAC:
  - Will ask the consumer only for the minimum amount of PII necessary to help.
  - 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 into coverage after first meeting with the consumer if the consumer provides his or her contact information.
  - Might share the consumer's PII if referring consumer to another source of help.
  - Will provide the consumer with copies of the completed authorization form and the Navigator's or CAC's roles and responsibilities in Attachment A.
- It also provides space to tell consumers about any state requirements that require use of consumer PII.

23



Remember: these suggestions are not intended to replace your obligation to determine how to follow the specific privacy and security standards that apply to your work, and the suggestions in this document might not be necessary in all circumstances, or you might have to do more than what is suggested here in order to meet the privacy and security standards that apply to your work. The specific privacy and security standards that apply to your work are contained in your organization's agreement with CMS or the terms and conditions for your grant or contract with CMS, as applicable.



Any copies you make or retain of consumers' official documents, like all PII, should be kept in a secure place and in a manner consistent with the privacy and security standards that apply to you.

4. Best Practices for Handling PII, *cont'd*

FFM Navigator and CAC organizations must implement policies and procedures to handle PII breaches and security incidents consistent with CMS' Incident Handling and Breach Notification Procedures.

CMS

26

Breach is defined by OMB Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information (May 22, 2007), as the compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, loss of control or any similar term or phrase that refers to situations where persons other than authorized users or for other than an authorized purpose have access or potential access to Personally Identifiable Information (PII), whether physical or electronic.

Incident, or Security Incident, means the act of violating an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

4. Best Practices for Handling PII, *cont'd*

Such policies and procedures must:

- Identify personnel responsible for reporting and managing Incidents or Breaches involving PII to CMS and require these personnel to be available to CMS upon request.
- Address how to identify an incident.
- Address how to determine if PII is involved in an incident.
- Require all CACs or Navigators to report potential incidents and 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.

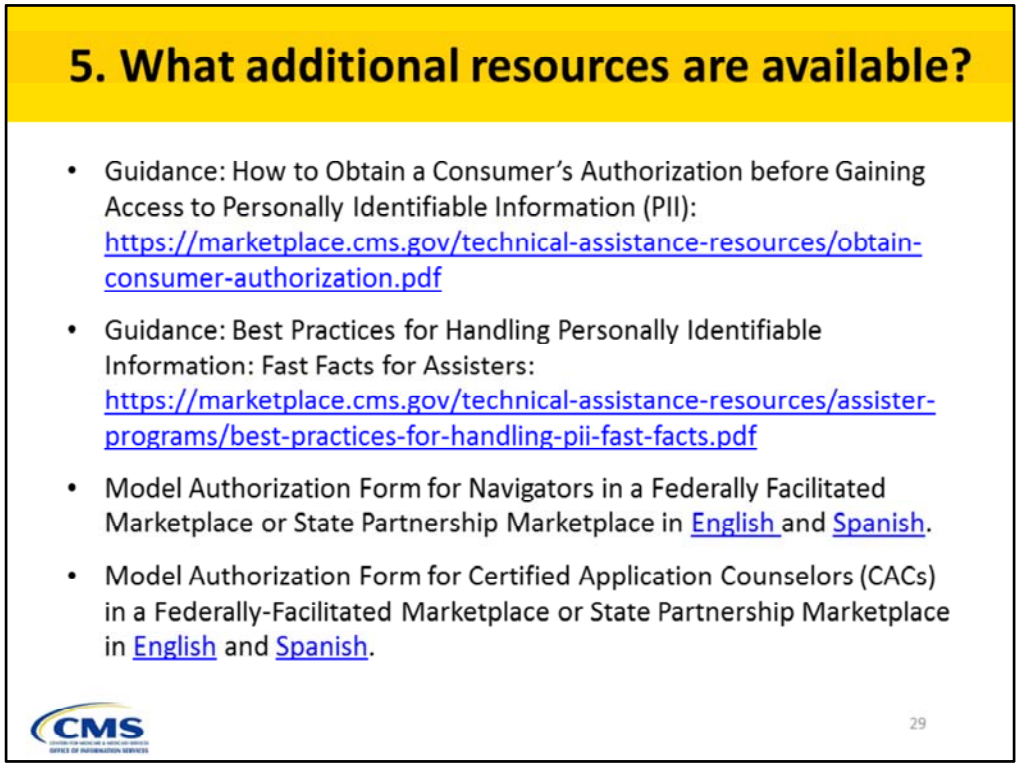
27

4. Best Practices for Handling PII, *cont'd*

Examples of issues you should report include:

- Lost, stolen, or misplaced records containing PII
- Unauthorized persons accessing or taking possession of consumer PII
- Lost, stolen, or misplaced electronic devices (e.g., tablets or laptops) that contain consumer PII
- Any other unauthorized disclosure of PII.

28



Please note that the document *Guidance: Best Practices for Handling Personally Identifiable Information: Fast Facts for Assisters* pre-dates the most recent FFM Navigator and CAC privacy and security standards located in Navigators' grant terms and conditions and certified application counselor designated organizations' agreements with CMS. FFM Navigators and CACs may refer to this guidance for tips and best practices, but must adhere to the privacy and security standards in their grant terms and conditions or agreements with CMS. We are in the process of updating this guidance.

5. What additional resources are available? *cont'd*

- As always, If you have questions about privacy and security requirements, you should direct your questions to:
  - **Certified application counselors and non-Navigator assistance personnel**: CACQuestions@cms.hhs.gov
  - **Navigators**: NavigatorGrants@cms.hhs.gov
  - **CMS contractors**: contact appropriate CMS personnel
- **Reporting incidents or breaches**: Contact **CMS IT Service Desk** (available 24 hours a day, 7 days a week) within on hour after discovery of the breach:

  Phone: **410-786-2580** or **1-800-562-1963**

  Email: CMS_IT_Service_Desk@cms.hhs.gov

30