Requirements and Best Practices for Assisters on Providing Remote Consumer Assistance

This job aid provides information and guidance Navigators and certified application counselors (CACs) (collectively, assisters) need to know in order to provide remote help securely to consumers applying for and enrolling in Marketplace coverage.

Overview

Effective June 18, 2018, Navigators in Federally-facilitated Marketplaces (FFMs, also known as Federally-facilitated Exchanges, or FFEs) are not required to maintain a physical presence in their Marketplace service area. In some cases, Navigators may provide remote application assistance (e.g., online or by phone), provided that such assistance is permissible under their organization's contract, grant terms and conditions, and agreement with CMS and/or their organization.

CACs in FFMs may also provide remote application assistance if such assistance is permitted by their certified application counselor designated organization (CDO).

Given the challenges associated with the COVID-19 pandemic, we encourage the assister community to provide consumers with the best enrollment assistance they can, consistent with their duties as assisters. The following sections discuss both rules and best practices for providing remote Marketplace application and enrollment assistance.

For other general information about COVID-19, visit:

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

- CDC.gov/coronavirus for the latest COVID-19-related preventive practices and any applicable state and local guidance.
- CMS CCIIO Coronavirus Disease 2019 (COVID-19) Guidance
- COVID-19 Fast Facts for Assisters

Privacy Practices

Whether you are helping consumers in person, over the phone, or online, remember that you must always obtain consumers' consent prior to accessing their personally identifiable information (PII). The FFMs establish assister privacy and security standards through agreements with "non-Exchange entities" such as Navigator grantees and CDOs. Individual CACs in an FFM should refer to their agreements with their CDOs since these agreements must include the privacy and security standards established by the FFMs. Protecting consumers' PII should be routinely discussed and monitored within your organization, and continuing education is strongly encouraged.

Records of consumer authorization must be appropriately secured and retained for at least six years, in accordance with federal regulations, unless a longer period is required by other applicable law. Consumers can revoke or limit their authorization at any time.

For guidance on receiving consumers' consent and protecting PII, visit Requirements and Best Practices for Assisters on Handling Personally Identifiable Information.

For guidance on obtaining consumers' consent remotely over the phone, visit How to Obtain a Consumer's Authorization Before Gaining Access to Personally Identifiable Information.

For guidance on using HIPAA-compliant cloud-based storage, visit HHS Guidance on HIPAA & Cloud Computing.

Navigator and CAC Security Requirements

Navigators and CACs in FFMs are permitted to create, collect, disclose, access, maintain, store, and use consumer PII to the extent necessary for purposes related to their required or authorized assister functions (referred to in their agreements as "authorized functions").

The FFM Navigator and CAC privacy and security requirements address how you should handle PII when performing your required or authorized duties. Check your grant terms and conditions or agreement to identify which types of functions are authorized functions. Some of these functions are different depending on whether you are a Navigator or a CAC.

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

- Consumers' information is accurate.
- Information is used only when necessary and relevant to the activity at hand.
- Consumers know and agree to all uses of information.
- Appropriate, swift action is taken when an incident or breach occurs.
- Confidentiality is protected to comply with all applicable laws and create trust between assisters and consumers.

Assisters are permitted (but not required) to contact consumers to offer assistance with annual Marketplace eligibility redetermination and re-enrollment processes if a consumer already provided their consent to an assister to follow up with the consumer.

Obtaining and Storing Electronic Records of Consumers' Consent

You and your organization are required by federal regulations to maintain a record of each consumer authorization obtained. The regulations do not prescribe a standard format or process for obtaining the authorization or for maintaining its record, so assisters have flexibility to determine how they will maintain such a record. However, CMS has developed model consumer authorization forms that assisters may adopt or modify. If in electronic format, we recommend that the authorization be kept in a password-protected computer and/or a file that is kept secure at all times. Only those personnel who need to access the records to carry out their duties and responsibilities should be given access to them. In addition, CMS expects that each assister organization establishes internal policies and procedures to keep each record of authorization secure and organized in a way that allows a consumer to request access to his or her authorization and make corrections as needed. For example, CMS recommends that each assister service location maintain a central repository that contains each record of authorization collected from each consumer seeking services at that location.

As best practices for protecting consumer PII electronically, assisters **should:**

- Restrict access so only authorized individuals have access to PII.
- Make sure that all scanning and copying equipment that may be used doesn't electronically retain copies of the images.
- Securely store PII collected from a consumer, including name, email address, telephone number, application ID number, addresses, or other notes.

- Verify that “auto-fill” settings on your internet browsers are turned off, and recommend that consumers follow the same steps, especially if they are using public or shared devices.
- Maintain computer security, including the use of a secure wireless network, when performing assistance using an authorized mobile device (for example, a tablet).
- Protect emails that contain PII (for example, use encryption).
- Lock up portable devices (for example, laptops or cell phones).
- Clear your web browser history to avoid other users accessing PII.
- Securely store PII in a password-protected file on a password-protected computer to which only authorized individuals have access.

Additionally, assisters **should not:**

- Store sensitive consumer data on any computer with an internet connection unless it’s essential for conducting your business.
- Send or forward emails with PII to personal email accounts (for example, Yahoo or Gmail).
- Upload PII to unauthorized websites (for example, wikis).
- Use unauthorized mobile devices to access PII.
- Access, use, or disclose the consumer’s PII for reasons not clearly directly related to the assister’s regulatory duties.
- Request any information that is not immediately necessary to complete an application.

If you work with other organizations in your work with the FFM, you remain legally bound to and responsible for all obligations to protect consumers' PII. You are required to obligate the other organization to the same privacy and security standards that you must legally follow.

Providing Online Application Assistance Using Video Conference and Secure Screen Sharing Applications

CMS regulations do not provide standard guidelines for using secure screen sharing applications when providing online assistance to consumers. CMS does suggest that Navigator organizations and CDOs consider creating a specific plan for security when using screen sharing applications and share that security plan with their assisters and consumers.

Helpful Tips

When using screen sharing applications, there are both technical tools for creating a secure environment and behavioral techniques for ensuring information is protected. Technical tips include:

- Verify your security settings before each screen sharing session. These features are not always enabled by default. Consider creating a password to participate in the meeting and make sure it is not publicly discoverable or accessible.
- Make sure you are using the most up-to-date versions of any screen sharing software.
- Have only the relevant information visible on screen. Close or minimize any windows or applications that are not essential to the meeting.
- Pay attention to any links to screen sharing applications provided to you, and be wary of phishing and attempts from malicious actors to gain access to private information.

Communicating with consumers and paying attention to your physical environment can also ensure secure meetings:

- Monitor your physical environment before making yourself visible on screen. Make sure there is no private or secure information visible in the space around you.
- Before recording a session, secure the consumer's permission. Memorialize the consent at the beginning of the recorded session on the recording.
- Always keep in mind and follow requirements to obtain and document consent to receive PII and retain it for the required time period.

Assisters may find the following websites helpful and are strongly encouraged to review these links when using video conferencing tools as a means of assisting consumers.

Note: CMS is offering these links for informational purposes only and this fact should not be construed as an endorsement of the host organization's programs or activities.

- Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA.gov):
    - Tips for Video Conferencing

    - Guidance for Securing Video Conferencing[1]
    - Telework Guidance and Resources
        - CISA provides detailed guidance on telework, virtual technology, and device security. These resources can be particularly helpful if your organization has not yet created or is in the process of creating a plan around security in a telework and virtual communications environment.
- Federal Trade Commission (FTC) guidance for protecting consumers, businesses, and the public on avoiding online scams during the COVID-19 pandemic: FTC.gov/coronavirus

Helping Consumers who Experience Issues with the HealthCare.gov Website

Consumers may reach out to assisters for help if they are experiencing issues when creating, updating, or submitting their Marketplace applications. Many common problems can be avoided by following a few simple tips. Remind consumers who are applying online for Marketplace coverage that some web browsers offer a smoother experience than others. HealthCare.gov is compatible with most popular web browsing software. This includes the most recent and commonly used versions of Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, and Apple Safari. If a consumer is having problems using HealthCare.gov, like getting stuck or seeing pages displayed incorrectly, you may want to suggest the consumer make the following adjustments to their browser:

- Be sure the consumer is running the latest version of their browser.
- Have them set their browser to “accept cookies.”
- Remind them to clear their “cache” and cookies when finished.

You can also direct consumers to call the Marketplace Call Center at 1-800-318-2596 (TTY: 1-855-889-4325) for assistance. For more information, visit How Assisters Can Help Consumers Apply for Coverage through the Marketplace Call Center.

For more information, visit:

- HealthCare.gov Browsers and Settings

[1] This link has a table listing the security settings of common video conferencing and screen sharing applications.

- The Assister's Roadmap to Resources

Examples of How to Fulfill the Consumer Authorization Requirement when Providing Remote Assistance

Example 1—Assisting a Homebound Consumer over the Telephone

Scenario: You are assisting a consumer for the first time. The consumer is homebound, and you are providing assistance over the telephone.

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. 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.

Example 2—Consumer Makes Initial Contact and Shares PII

Scenario: 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 likely contains the consumer's PII.

Authorization: If a consumer directly contacts you or your organization for assistance and provides their PII, you still must 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 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.

Additional Resources

- Privacy, Security, and Fraud Prevention Standards WBT Course
- Privacy and Security Standards for Navigator Cooperative Agreement Recipients (beginning on page 7)
- SOP Consumer Protections: Privacy and Security Guidelines
- SOP Consumer Protections: Fraud Prevention Guidelines
- SOP 1 – Receive Consent Before Accessing Consumer PII
- Obtaining Consumer Authorization and Handling Consumers' Personally Identifiable Information (PII) in the Federally-facilitated Marketplace