Requirements and Best Practices for Assisters on Providing Remote Consumer Assistance

This job aid provides information and guidance for Navigators, Certified Application Counselors (CACs), and Enrollment Assistance Personnel (EAPs) (collectively, assisters) when providing remote assistance to consumers applying for and enrolling in the Federally-facilitated Marketplace (FFM) coverage. It's important that assisters are familiar with any other specific requirements on this topic that may be included as part of their CMS-funded Navigator cooperative agreement, CMS-CDO (CAC designated organizational) agreement, or EAP contract.

Table of Contents

Version 2.0. July 2024. This information is intended only for the use of entities and individuals certified to serve as Navigators, certified application counselors, or non-Navigator assistance personnel in a Federally-facilitated Marketplace. The terms "Federally-facilitated Marketplace" and "FFM," as used in this document, include FFMs where the state performs plan management functions. Some information in this manual may also be of interest to individuals helping consumers in State-based Marketplaces and State-based Marketplaces using the Federal Platform. This material was produced and disseminated at U.S. tax filer expense.

Overview

Although it's no longer required that assisters, specifically Navigators, maintain a physical presence in the FFMs, the most successful assisters do, and some even live in the communities they serve. Especially in rural and hard-to-reach areas, assisters may provide remote application assistance either online or by phone, for example.

PII and Privacy Practices

Whether you are helping consumers in person or remotely, you must always obtain consumers' consent **prior to** accessing their personally identifiable information (PII). You must also comply with all privacy and security standards through your respective agreement or contract with CMS.

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. You must strictly adhere to all applicable privacy and security terms and conditions to ensure that consumer PII is properly collected, used, stored, and safeguarded. Your organization's leadership or designated person(s) must let you know what these requirements are to ensure that you understand and comply with all PII and privacy and security standards, including any applicable organizational policies and procedures.

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 must be told that they can revoke or limit their authorization at any time.

For guidance on receiving consumers' consent remotely over the phone, visit Obtaining Consumer Authorization and Handling Consumers' PII in the FFM webinar.

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

Best Practices Protecting PII Assisting Consumers Remotely

Here are best practices for protecting consumer PII electronically**:**

- Make sure that all scanning, faxing, and copying equipment used doesn't retain copies of the images or information.
- 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 by encrypting them, for example.
- Lock up portable devices (for example, laptops or cell phones) and don't keep them unattended in your vehicle, a hotel room, or the like.
- Routinely 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 within your organization have access.

Assisters **should not:**

- Store or input sensitive consumer data on any electronic devices using an unsecure internet connection like in a hotel, restaurant, café, business, or the like.
- Give or share documentation (emails, notes, etc.) that contain a consumer's PII or discuss a consumer's PII with anyone.
- Upload PII to unauthorized websites (for example, wikis).
- Use unauthorized mobile or other electronic devices to access, store, or use consumers' PII.
- Access, use, or disclose the consumers' PII for reasons unrelated to the assister's regulatory duties.
- Request any information that is not necessary to complete an application.

If assisters work with other organizations in their work with the FFM, they remain legally bound to and responsible for all obligations to protect consumers' PII.

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. However, CMS does suggest that assister organizations should consider creating a specific plan for privacy and security requirements when using screen sharing applications.

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 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 to use the most up-to-date versions of any screen sharing software.
- Have only the relevant information visible on the screen (be also aware of what's in the background). Close or minimize any windows or applications that are not essential to the meeting.
- Pay attention to any links to screen sharing applications provided, and be wary of phishing and attempts from malicious actors to gain access to private information.

Behavioral tips:

- Communicating with consumers and paying attention to the physical environment you're in can also ensure secure meetings:
    - Monitor the physical environment before becoming visible on the screen and during your remote assistance. Make sure that no one can access or see your screen or hear your conversation with the consumer.
    - Before starting a session, make sure that the consumer is comfortable in that setting and gives consent.
- Always keep in mind and follow the requirements to obtain, use, document, store, and safeguard consumer PII.

Assisters may find the following websites helpful from the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA). 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:

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.

- Tips for Video Conferencing
- Guidance for Securing Video Conferencing[i]
- Telework Guidance and Resources

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, assisters 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.

Assisters 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
- The Assister's Roadmap to Resources

Additional Resources

Note: CMS offers these links for informational purposes only, and inclusion of these websites shouldn't be construed as an endorsement of any third-party organization's programs or activities.

For more information visit:

- Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency: CISA.gov/
- Guidance for Securing Video Conferencing: CISA.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.pdf
- HealthCare.gov Browsers and Settings: Healthcare.gov/tips-and-troubleshooting/browsers-and-settings/
- HHS Guidance on HIPAA & Cloud Computing: HHS.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html
- How Assisters Can Help Consumers Apply for Coverage through the Marketplace Call Center: CMS.gov/marketplace/technical-assistance-resources/helping-consumers-apply-through-the-call-center.pdf
- How to Obtain a Consumer's Authorization Before Gaining Access to Personally Identifiable Information: CMS.gov/marketplace/technical-assistance-resources/obtain-consumer-authorization.pdf
- Model Consumer Authorization Forms: CMS.gov/marketplace/technical-assistance-resources/model-auth-form-template-for-cacs-english.pdf
- Obtaining Consumer Authorization and Handling Consumers' Personally Identifiable Information (PII) in the Federally-facilitated Marketplace: CMS.gov/marketplace/technical-assistance-resources/consumer-authorization-and-handling-pii.pdf
- Privacy and Security Standards for Navigator Cooperative Agreement Recipients (beginning on page 7): CMS.gov/cciio/programs-and-initiatives/health-insurance-marketplaces/downloads/example-2018-privacy-security-terms-conditionspdf.pdf
- Privacy, Security, and Fraud Prevention Standards WBT Course: CMS.gov/marketplace/technical-assistance-resources/training-materials/privacy-security-and-fraud-prevention.pdf

- Requirements and Best Practices for Assisters on Handling Personally Identifiable Information: CMS.gov/marketplace/technical-assistance-resources/assister-programs/best-practices-for-handling-pii-fast-facts.pdf
- Telework Guidance and Resources: CISA.gov/topics/risk-management/coronavirus/telework-guidance-and-resources
- The Assister's Roadmap to Resources: CMS.gov/marketplace/technical-assistance-resources/assisters-roadmap-to-resources.pdf
- Tips for Video Conferencing: CISA.gov/sites/default/files/publications/CISA_Video_Conferencing_Tips_S508C.pdf

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