CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Part II: Marketplace Privacy & Security Requirements for Agents and Brokers

June 21, 2018

Centers for Medicare & Medicaid Services (CMS)
Center for Consumer Information & Insurance Oversight (CCIIO)

Disclaimer

The information provided in this presentation is intended only as a general informal summary of technical legal standards. It is not intended to take the place of the statutes, regulations, 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, and other interpretive materials for complete and current information about the requirements that apply to them.

This document generally is not intended for use in the State-based Marketplaces (SBMs) that do not use HealthCare.gov for eligibility and enrollment. Please review the guidance on our Agents and Brokers Resources webpage (http://go.cms.gov/CCIIOAB) and Marketplace.CMS.gov to learn more.

Unless indicated otherwise, the general references to "Marketplace" in the presentation only includes Federally-facilitated Marketplaces (FFMs) and State-based Marketplaces on the Federal Platform (SBM-FPs).

This communication was printed, published, or produced and disseminated at U.S. taxpayer expense.

Webinar Agenda

- Background/Previous Webinars
- Review of Requirement to Provide a Privacy Notice Statement
- Review of Required Security Controls
- Key Reminders and Resources
- Other Marketplace Updates
- Questions and Answers

Background

- This presentation is a follow on to the September 27, 2017 webinar on *Marketplace Privacy & Security Requirements for Agents and Brokers*, which is available on the [Resources for Agents and Brokers webpage](#).
- Topics covered in this resource include:
  - Key Sources for Agent and Broker Requirements
  - Requirement for Privacy Notice Statement
  - Requirement to Obtain Consumer Consent Prior to Assistance
  - Providing Correct Information to the Marketplace
  - Authorized Functions for Use of Personally Identifiable Information (PII)
  - Best Practices to Manage Risks to Information Security
  - Reporting an Incident or Breach of PII

Background

- Also be sure to review the presentation from the May 24, 2018 webinar on *Compliance with Marketplace Requirements: Considerations for Agents and Brokers*, which is available on the [Resources for Agents and Brokers webpage](#) .

- Topics covered in this resource include:
  - Requirement to Obtain Consumer Consent Prior to Assistance
  - Assisting Consumers Who Do Not Have an Email Address
  - Assisting Consumers Who May Qualify for Medicare Coverage
  - How to Report Potentially Fraudulent Activity

PII Definition

- 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.
- Section II(b) of the Individual Marketplace Privacy and Security Agreement and the Small Business Health Options Program (SHOP) Privacy and Security Agreement specifies the types of PII that an individual may encounter in performing the role of an agent or broker in the Marketplace.
- Examples of PII include name, Social Security number, address, email address, and date of birth.

* See Office of Management and Budget Memoranda M-17-12 (January 3, 2017)

CENTERS FOR MEDICARE & MEDICAID SERVICES

Part II: Marketplace Privacy & Security Requirements for Agents and Brokers

Review of Requirement to Provide a Privacy Notice Statement

Provision of Privacy Notice Statement

- Prior to collecting PII, you must provide a Privacy Notice Statement that is prominently displayed:
  - On a public-facing website, if applicable, or
  - On the electronic and/or paper form used to gather and/or request PII.
- The statement must be written in plain language and provided in a manner that is accessible and timely to people living with disabilities and with limited English language proficiency.
- Failure to comply with the Privacy Notice Statement requirement could result in termination of your Agreement(s) with CMS and registration with the Marketplace.
- The Individual Marketplace Privacy and Security Agreement and the SHOP Privacy and Security Agreement have more information about the Privacy Notice Statement.

Content of Privacy Notice Statement

- The statement must contain, at a minimum, the following information (you should substitute the underlined content in brackets with content that is specific to your operations):

Privacy Notice Statement
We are authorized to collect personally identifiable information (PII) from you by [legal authority to collect PII]. Any PII we collect is used to [purpose of the information collection]. If you choose to give us PII, we may share this information with [to whom PII might be disclosed, and for what purposes]. PII is used or disclosed only under the following circumstances: [authorized uses and disclosures of any collected information]. [Indicate whether the request to collect PII is voluntary or mandatory under the applicable law]. If you choose not to provide us with the PII requested, or not to respond to certain questions, [effects of non-disclosure if an individual chooses not to provide the requested information].

- The statement should inform applicants that information they provide will be submitted to CMS (a federal agency) and will be maintained in a federal System of Records.

Myths and Facts about the Privacy Notice Statement

Myth

Clients must sign the Privacy Notice Statement.

Myths and Facts about the Privacy Notice Statement

Myth

Clients must sign the Privacy Notice Statement.

Fact

NOT TRUE! Consumers do not need to sign the Privacy Notice Statement. You must provide it to your clients by either conspicuously displaying it on a public facing website or including it on the electronic and/or paper form used to gather and/or request PII.

Myths and Facts about the Privacy Notice Statement

Myth

The Privacy Act Statement that consumers view at HealthCare.gov satisfies the requirement that I provide my clients a Privacy Notice Statement.

HealthCare.gov

Español

Get Coverage | Keep or Update Your Plan | See Topics | Get Answers | Search

Privacy Act Statement

Permission for information submitted

By submitting this application, you represent that you have permission from all of the people whose information is on the application to both submit their information to the Marketplace, and receive any communications about their eligibility and enrollment.

Privacy Act Statement – effective 10/1/2013

We are authorized to collect the information on this form and any supporting documentation, including social security numbers, under the Patient Protection and Affordable Care Act (Public Law No. 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law No. 111-152), and the Social Security Act.

We need the information provided about you and the other individuals listed on this form to determine eligibility for: (1) enrollment in a qualified health plan through the Federal Health Insurance Marketplace, (2) insurance affordability programs (such as Medicaid, CHIP, advance payment of the premium tax credits, and cost sharing reductions), and (3) certifications of exemption from the individual responsibility requirement. As part of that process, we will verify the information provided on the form, communicate with you or your authorized representative, and eventually provide the information to the health plan you select so that they can enroll any eligible individuals in a qualified health plan or insurance affordability program. We will also use the

Myths and Facts about the Privacy Notice Statement

Myth

The Privacy Act Statement consumers view at HealthCare.gov satisfies the requirement that I provide my clients a Privacy Notice Statement.

Fact

NOT TRUE! Your Privacy Notice Statement must be tailored to describe your privacy practices and include all of the required minimum information described on Slide 9.

Myths and Facts about the Privacy Notice Statement

Myth

Prior to assisting any Marketplace client, I must provide both the Privacy Notice Statement and obtain the client's consent to my assistance.

Myths and Facts about the Privacy Notice Statement

Myth

Prior to assisting any Marketplace client, I must provide both the Privacy Notice Statement and obtain the client's consent to my assistance.

Fact

TRUE! The Privacy Notice Statement must be provided <u>and</u> the consumer must give consent prior to you collecting the consumer's PII or helping the consumer apply for financial help and/or enrolling in a Marketplace qualified health plan (QHP).

Comparison of Privacy Notice Statement and Consumer Consent

	Privacy Notice Statement	Consumer Consent
When?	Prior to collecting the consumer's PII	Prior to collecting PII and providing assistance in applying for financial help and/or enrolling in a Marketplace QHP
Signature Required?	No	No
Model Notice Available?	No	No
Required Content?	• Legal authority to collect PII • Purpose of the information collection; • To whom PII might be disclosed, and for what purposes • Authorized uses and disclosures of any collected information • Whether the request to collect PII is voluntary or mandatory under the applicable law • Effects of non-disclosure if an individual chooses not to provide the requested information	• Should acknowledge that you have informed the client of the functions and responsibilities that apply to your role in the Marketplace • Should include the following: - The client's name - The date the consent was given - The name of the agent(s) or broker(s) to whom consent was given (Note that this could include additional names of agents or brokers if the consenter authorized multiple agents or brokers within the same organization)
Source of Requirement?	Individual Marketplace Privacy and Security Agreement and SHOP Privacy and Security Agreement	Agent and broker standards of conduct: 45 CFR § 155.220(j)(2)

CENTERS FOR MEDICARE & MEDICAID SERVICES

Part II: Marketplace Privacy & Security Requirements for Agents and Brokers

Review of Required Security Controls

Security Controls

- To protect consumer PII throughout the year, you must establish and implement operational, technical, administrative, and physical safeguards that ensure that:
  - PII is only used by or disclosed to those authorized to receive or view it;
  - 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; and
  - PII is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with CMS retention requirements.
- You are also responsible for ensuring that members of your workforce who have a need for consumer PII to perform their duties strictly follow these safeguards.

Security Controls (Continued)

- You must monitor, periodically assess, and update your security controls and related system(s) to ensure the continued effectiveness of those controls.
- You must also develop and utilize secure electronic interfaces when transmitting PII electronically.

Scenario: Sharing Passwords

Your colleague Adam has not yet set up his account and asks you for your password so he can access the Direct Enrollment(DE) Pathway for Best Health Insurance to assist one of his clients.

Should you provide Adam with your log in credentials?

A. Yes. Adam is a member of your workforce so it does not matter if he can access your clients' PII that is stored in the Best Health Insurance system, and if Adam enrolls his client using your password, your National Producer Number (NPN) will be recorded on the application so you will earn the commission for that enrollment.
B. No. You should NEVER share your password with anyone.

Scenario: Sharing Passwords Answer

Your colleague Adam has not yet set up his account and asks you for your password so he can access the DE Pathway for Best Health Insurance to assist one of his clients.

Should you provide Adam with your log in credentials?

A. Yes. Adam is a member of your workforce so it does not matter if he can access your clients' PII that is stored in the Best Health Insurance system, and if Adam enrolls his client using your password, your NPN will be recorded on the application so you will earn the commission for that enrollment.

B. No. You should NEVER share your password with anyone.

Scenario: Sharing Passwords Answer (Continued)

- Even though Adam is a member of your workforce, he does not have a need for your clients' PII to perform his duties.
- Financial considerations (e.g., commission payments) should never supersede compliance with the Marketplace privacy and security requirements.

Scenario: Sharing PII via Email

Your organization keeps a master database of all its Marketplace clients that contains client names, application numbers, application history, and contact information. You are finishing up another busy day during the Marketplace Open Enrollment period and need to send an email with this information for the clients you assisted today to Sue, who maintains the database.

What steps must you take to ensure that you are protecting your clients' PII and complying with the required security controls?

A. Ensure that the Privacy Notice Statement that you provide your clients explains that their PII is shared with authorized members of your workforce for the purpose of maintaining the contact database.
B. Attach your client tracking spreadsheet to the email to Sue.
C. Copy the rows from your client tracking spreadsheet and paste them in the body of the email to Sue.
D. Encrypt your client tracking spreadsheet prior to attaching it to the email to Sue.

Scenario: Sharing PII via Email Answer

Your organization keeps a master database of all its Marketplace clients that contains client names, application numbers, application history, and contact information. You are finishing up another busy day during the Marketplace Open Enrollment period and need to send an email with this information for the clients you assisted today to Sue, who maintains the database.

What steps must you take to ensure that you are protecting your clients' PII and complying with the required security controls?

A. **Ensure that the Privacy Notice Statement that you provide your clients explains that their PII is shared with authorized members of your workforce for the purpose of maintaining the contact database.**

B. Attach your client tracking spreadsheet to the email to Sue.

C. Copy the rows from your client tracking spreadsheet and paste them in the body of the email to Sue.

D. **Encrypt your client tracking spreadsheet prior to attaching it to the email to Sue.**

Scenario: Sharing PII via Email Answer (Continued)

- Remember to include a description of to whom PII might be disclosed, and for what purposes, in your Privacy Notice Statement.
- Ensure communications are encrypted when exchanging PII or other sensitive data electronically.
  - Encryption protects the confidentiality of the email by scrambling the message, thus requiring a password to decrypt the message.
  - Encrypting email attachments also protects them from being compromised on unencrypted servers.
- Sending passwords via email is not recommended. At a minimum, do not send the password in the same email as the encrypted file. Suggested methods of password transmittal include text message, phone conversation, predetermined shared secrets, or a shared file system (e.g., SharePoint).

Scenario: Safeguarding Against Threats

Sue stores your organization's master Marketplace client database on a shared network server. Which of the following are safeguards that should be implemented to ensure your clients' PII stored on this server is protected against any reasonably anticipated threats or hazards to its confidentiality, integrity, and availability?

A. Ensure that all computers used to access the server are regularly updated with the latest security software to protect against network attacks and penetration attempts.
B. Limit physical access to secured areas where there are information systems that contain consumer PII to authorized personnel via appropriate authorization credentials (e.g., identification badges, proximity cards, smart cards).
C. Use caution when connecting any wireless device (e.g., laptop) to a public wireless network, and only use secure, trusted wireless access points.
D. Require regular privacy and security awareness and training programs for all members of your workforce who have access to client PII.

Scenario: Safeguarding Against Threats Answer

Sue stores your organization's master Marketplace client database on a shared network server. Which of the following are safeguards that should be implemented to ensure your clients' PII stored on this server is protected against any reasonably anticipated threats or hazards to its confidentiality, integrity, and availability?

A. **Ensure that all computers used to access the server are regularly updated with the latest security software to protect against network attacks and penetration attempts.**

B. **Limit physical access to secured areas where there are information systems that contain consumer PII to authorized personnel via appropriate authorization credentials (e.g., identification badges, proximity cards, smart cards).**

C. **Use caution when connecting any wireless device (e.g., laptop) to a public wireless network, and only use secure, trusted wireless access points.**

D. **Require regular privacy and security awareness and training programs for all members of your workforce who have access to client PII.**

Part II: Marketplace Privacy & Security Requirements for Agents and Brokers

Key Reminders and Resources

Points to Remember

- Provide a Privacy Notice Statement to all Marketplace clients prior to collecting their PII.
- Tailor your Privacy Notice Statement to ensure it contains the required information (see Slide 9 or Standard 2a of the Marketplace Privacy and Security Agreement).
- Ensure your office establishes and implements operational, technical, administrative, and physical safeguards that effectively protect your Marketplace clients' PII throughout the year.
- Ensure that all members of your workforce who have a need for consumer PII to perform their duties strictly follow these safeguards.

Key Source for Agent and Broker Privacy Standards

- The specific privacy standards for agents and brokers are described in Appendix A of the Agreement(s) with CMS, which you execute annually as part of Marketplace registration.
  - Individual Marketplace Privacy and Security Agreement
  - SHOP Privacy and Security Agreement
- You should review these privacy standards and CMS' eight privacy principles in [45 CFR § 155.260(a)(3)]() to understand the limits on how you may use any information gained as part of providing assistance to a qualified individual.
- You may only collect, use, or disclose PII to the extent necessary to carry out the authorized functions outlined in these Agreements, unless you obtain the specific, written consent of the consumer.

Please carefully read the following Agreement and Appendices, which are incorporated by reference into the Agreement. By clicking "I Agree" when this option is made available to you, you understand this constitutes your electronic signature and you accept/agree to be bound by and abide by the terms and conditions of the Agreement. If you do not want to accept/agree to the terms and conditions of the Agreement, you must click "I Do Not Agree".

You can access the Appendices to this Agreement by clicking on the following links:

[Appendix A]()

[Appendix B]()

AGREEMENT BETWEEN AGENT OR BROKER AND THE CENTERS FOR MEDICARE & MEDICAID SERVICES FOR THE FEDERALLY-FACILITATED EXCHANGE INDIVIDUAL MARKET

THIS AGREEMENT ("Agreement") is entered into by and between THE CENTERS FOR MEDICARE & MEDICAID SERVICES ("CMS"), as the Party (as defined below) responsible for the management and oversight of the Federally-facilitated Exchange* ("FFE"), including the CMS Data Services Hub ("Hub"), and the agent, broker, or entity who established this account and whose name appears on the Marketplace Learning Management System (MLMS) account (hereinafter referred to as "ABE"), an Agent or Broker that, among other things, assists Consumers, Applicants, Qualified Individuals and Enrollees in applying for Advance Payments of the Premium Tax Credits ("APTCs") and Cost-sharing Reductions ("CSRs") for Qualified Health Plans ("QHPs"), and/or in completing enrollment in QHPs offered in the individual market through the FFE, and provides Customer Service (CMS and ABE hereinafter referred to as "Party", or collectively, as the "Parties").

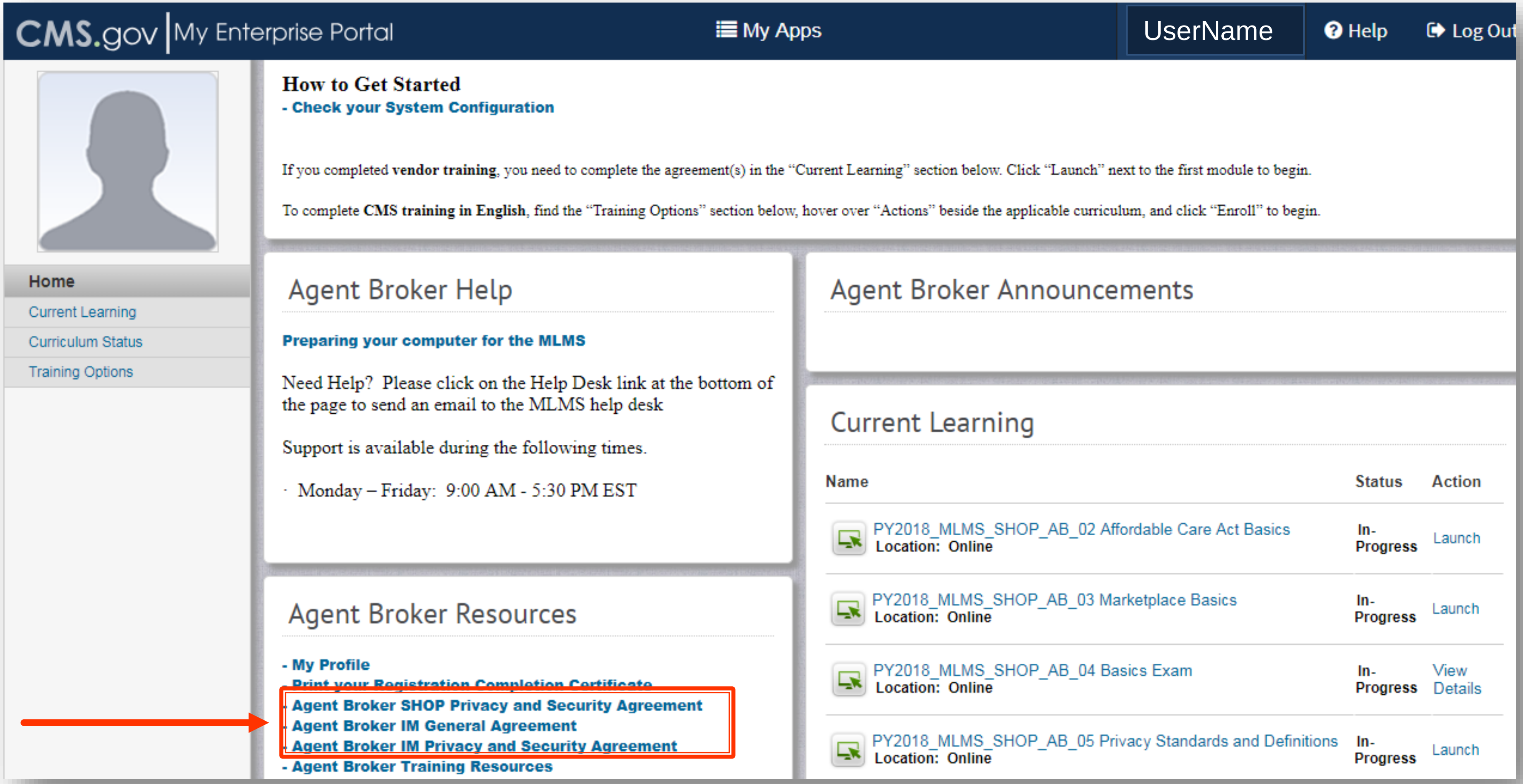
***References to the Federally-facilitated Exchange equates to the Federally-facilitated Marketplace**

WHEREAS:

1. Section 1312(e) of the Affordable Care Act ("ACA") provides that the Secretary of the U.S. Department of Health and Human Services ("HHS") shall establish procedures that permit Agents and Brokers to enroll Qualified Individuals in QHPs through an Exchange, and to assist individuals in applying for Advance Payments of the Premium Tax Credit ("APTCs") and Cost-sharing Reductions ("CSRs"), to the extent allowed by States. To participate in an FFE, Agents and Brokers must complete all necessary registration and training requirements under 45 CFR 155.220.
2. To facilitate the operation of the FFE, CMS desires to permit ABE to create, collect, disclose, access, maintain, store, or use their Personally Identifiable Information ("PII") from CMS, Consumers, Applicants, Qualified Individuals and Enrollees, or their legal

Where to Find the Privacy and Security Agreement

You can access the Marketplace Agreements at any time on the Marketplace Learning Management System (MLMS) Landing Page (via the [CMS Enterprise Portal]()).



Part II: Marketplace Privacy & Security Requirements for Agents and Brokers

Other Marketplace Updates

Upcoming Activities

- The slides from this webinar are already available on the Registration for Technical Assistance Portal (REGTAP) at www.REGTAP.info and will be available on the Resources for Agents and Brokers webpage in the coming days.
- Watch your email for invitations to upcoming webinars.

TOMORROW

Upcoming Assister Webinar*
June 22, 2:00-3:00 PM ET
Agents/Brokers Welcome!

- Medicaid and CHIP Overview

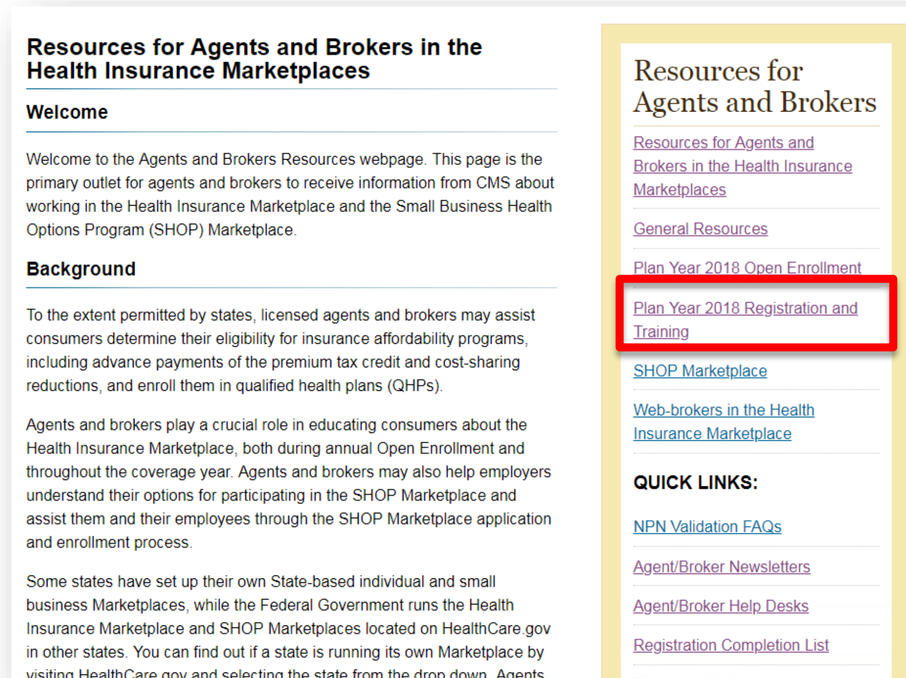
Upcoming Assister Webinar*
July 6, 2:00-3:30 PM ET
Agents/Brokers Welcome!

- Special Enrollment Periods
- Enrolling Young Adults and Other Hard to Reach Populations

*Webinar dates and topics are subject to change. CMS will share current webinar information via email.

Reminder: Complete Plan Year 2018 Agent and Broker Training

- Plan year 2018 Marketplace agent and broker registration and training is still available on the CMS Enterprise Portal.
- For a detailed description of the requirements and how to complete the registration steps, please select one of the following hyperlinks to download a helpful guide:
  - Guide to Plan Year 2018 Marketplace Registration and Training for New Agents and Brokers
  - Guide to Plan Year 2018 Marketplace Registration and Training for Returning Agents and Brokers



- For more information, select the “Plan Year 2018 Registration and Training” link on the sidebar of the Agents and Brokers Resources webpage.

Marketplace Agent and Broker Compliance Points to Remember

- Obtain consent from each client you work with prior to assisting him or her.
- Obtaining a signed Broker of Record form from an issuer or state Department of Insurance satisfies the consumer consent requirement.
- Do not create or maintain access to a client's HealthCare.gov account or associated email account.
- Do not create or use dummy addresses in place of the consumer's email or mailing address.
- You may not log in to HealthCare.gov on a consumer's behalf (i.e., using the consumer's HealthCare.gov account).
- If a client may be eligible for Medicare, direct him or her to Medicare for a determination before you assist that client to enroll in a Marketplace QHP.
- If you suspect or identify potentially fraudulent activity, you can report your concerns to the Department of Health & Human Services (HHS) Office of Inspector General Hotline, the Federal Trade Commission, or the Agent/Broker Email Help Desk, depending on the situation.

Agent and Broker Resources

Resource	Description	Link
Agents and Brokers Resources webpage	Primary outlet for information about participating in the Health Insurance Marketplace	http://go.cms.gov/CCIIOAB
HealthCare.gov	Official site of the Health Insurance Marketplace used for researching health coverage choices, eligibility, and enrollment	https://www.healthcare.gov/
Marketplace information source for Agents and Brokers	Provides additional technical assistance resources about Marketplace eligibility, financial assistance, enrollment, and more	https://marketplace.cms.gov
CMS' eight privacy principles: 45 C.F.R. § 155.260(a)	Basis for the privacy and security standards and implementation specifications in the Marketplace Privacy and Security Agreement	https://www.ecfr.gov/cgi-bin/text-idx?SID=681793000949593ae1acc821445c709d&mc=true&node=se45.1.155_1260&rgn=div8

Agent and Broker Resources (Continued)

Resource	Description	Link
Registration Completion List	Public list of agents and brokers who have completed Marketplace registration; used by issuers to verify your eligibility for compensation for assisting with consumer enrollments	https://data.healthcare.gov/ffm_ab_registration_lists
Find Local Help	Tool available on HealthCare.gov that enables consumers to search for a local, Marketplace-registered agent or broker with an active licensure status in a valid health-related line of authority to assist with FFM enrollment	https://localhelp.healthcare.gov/
Help On Demand	A third-party service that connects consumers seeking assistance with Marketplace-registered, state-licensed agents and brokers in their area who can assist with Marketplace enrollment when the consumer is available	https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/Help-On-Demand.pdf
Agent and Broker NPNs	Provides a search function to determine the correct NPN to enter in your MLMS profile and on Marketplace applications	www.nipr.com/PacNpnSearch.htm

Most Frequently Used Agent/Broker Marketplace Help Desks and Call Centers

Name	Phone # and/or Email Address	Types of Inquiries Handled	Hours (Closed Holidays)
Direct Agent/ Broker Partner Line	855-788-6275 Note: Enter your NPN to access this line.	• Assist consumers with HealthCare.gov account password resets • Special enrollment periods not available on the consumer application • Individual Marketplace eligibility and enrollment issues	Mon–Sun 24 hours/day
Agent/Broker Email Help Desk	FFMProducer-AssisterHelpDesk@cms.hhs.gov	• General enrollment and compensation questions • Manual identity proofing/Experian issues • Escalated general registration and training questions (not related to a specific training platform) • Agent/Broker Registration Completion List issues • Find Local Help and Help On Demand issues • Report concerns that a consumer or another agent or broker has engaged in fraud or abusive conduct	Mon–Fri 8:00 AM–6:00 PM ET

For a full list of Agent/Broker Help Desks and Call Centers, see https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/Agent-Broker-Help-Desks.pdf.

Most Frequently Used Agent/Broker Marketplace Help Desks and Call Centers

Name	Phone # and/or Email Address	Types of Inquiries Handled	Hours (Closed Holidays)
Agent/Broker Training and Registration Email Help Desk	MLMSHelpDesk@cms.hhs.gov	• Technical or system-specific issues related to the agent/broker training and registration system (i.e., the MLMS) • User-specific questions about maneuvering in the MLMS site, or accessing training and exams	Mon–Fri 9:00 AM–5:30 PM ET
Marketplace Service Desk	855-CMS-1515 855-267-1515 CMS_FEPS@cms.hhs.gov	• CMS Enterprise Portal password resets and account lockouts • Login issues on the DE agent/broker landing page • Other CMS Enterprise Portal account issues or error messages • 501 Downstream Error message on HealthCare.gov website issues • General registration and training questions (not related to a specific training platform)	Mon-Fri 8:00 AM–8:00 PM ET

For a full list of Agent/Broker Help Desks and Call Centers, see https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/Agent-Broker-Help-Desks.pdf.

Acronym Definitions

Acronym	Definition
CCIIO	Center for Consumer Information and Insurance Oversight
CMS	Centers for Medicare & Medicaid Services
DE	Direct Enrollment
FFM	Federally-facilitated Marketplace
MLMS	Marketplace Learning Management System
NPN	National Producer Number
PII	Personally Identifiable Information
QHP	Qualified Health Plan
REGTAP	Registration for Technical Assistance Portal
SBM	State-based Marketplace
SBM-FP	State-based Marketplace on the Federal Platform
SHOP	Small Business Health Options Program