The Marketplace and Cybersecurity

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

May 18, 2022
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. 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 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 Agent and Broker 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 include 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.
Agenda

01 Maintaining Compliance

02 Consumer Consent

03 Information Security Overview

04 Identifying and Protecting Personally Identifiable Information (PII)

05 Identifying Cybersecurity Breaches

06 Cyber Hygiene and Preventing Cybersecurity Breaches

07 Responding to Cybersecurity Breaches

08 Remediying Cybersecurity Breaches
Maintaining Compliance: Key Reminders

» Agents and brokers who participate in the Marketplace must complete all applicable steps of the Marketplace training and registration process prior to assisting consumers with selecting and enrolling in qualified health plans (QHPs).

» Agents and brokers must also:
  o Provide correct information to consumers;
  o Provide correct consumer information (e.g., consumer name, date of birth, address, email address) to the Marketplace for verifying consumer identity and applying for QHP coverage;
  o Refrain from marketing or conduct that is misleading;
  o Obtain consent from each client you work with prior to assisting them with Marketplace coverage, including prior to searching for a current application using an approved Classic Direct Enrollment (DE)/Enhanced Direct Enrollment (EDE) website;
  o Protect consumers' personally identifiable information (PII); and
  o Identify and report suspicious activity or potentially fraudulent behavior you observe in relation to the Marketplace.

» Finally, agents and brokers must comply with applicable federal and state requirements, including licensing and appointment standards, system access terms and conditions, and conflicts of interest and confidentiality provisions.
Maintaining Compliance: Key Reminders

» Consumer HealthCare.gov accounts should only have the consumer’s (or his or her legally authorized representative’s) email, telephone number, and mailing addresses.
  
  o Never enter your own agent or broker professional or company email, telephone number, or mailing address on a consumer’s application. Do not maintain access to a client’s HealthCare.gov account or associated email account.
  
  o You should not create or use dummy addresses in place of the consumer’s email or mailing address. As a best practice, you should also avoid the use of disposable email addresses.

» Ensure your clients are reporting accurate income when completing or updating the eligibility application. Reinforce that it is in their best interest to report the **most accurate** income estimate, not the estimate that maximizes the amount of premium tax credit for which they may be eligible.
  
  o Only submit income projections the consumer has knowingly authorized and confirmed is accurate.
  
  o You **SHOULD** make sure consumers are aware of other insurance affordability programs they may qualify for based on their estimated income. If consumers may be eligible for Medicaid/CHIP based on the information in their eligibility application, you **SHOULD** direct them to the State Medicaid Agency, or other resources that can help them enroll in coverage.
Agents and brokers should only make updates to a consumer’s application/policy at the direction of the consumer. This includes but is not limited to:

- Conducting a search for consumer applications using an approved Classic DE/EDE website.
- Helping them apply for financial help and/or enrolling in a Marketplace QHP, including checking the status of their coverage and making updates throughout the year.
- Calling the Marketplace Call Center to ask about the status of a Marketplace enrollment or make consumer changes.

**Note:** This requirement is different from, and in addition to, the requirement that consumers must provide you their consent for any use or disclosure of their PII outside the scope of the Privacy Notice Statement and the Authorized Functions for an agent or broker in the Marketplace.
CMS does not prescribe a standard format or process for obtaining or documenting consumer consent, so you have flexibility to determine how you will meet the consent requirement.

- While CMS does not provide a form, or specify that a form has to be signed, you can use a Broker of Record form from an issuer or state Department of Insurance to satisfy this requirement.

- If you are providing assistance verbally (such as over the phone), you may obtain consent by reading a script that contains, at a minimum, the required elements, and you should record in writing that the required consent was obtained. Recording these phone conversations is a best practice.

- Additionally, you may obtain consent electronically (such as via email or text message) or in person.

- The consent should acknowledge that the agent or broker has informed the consumer of the functions and responsibilities that apply to the agent’s or broker’s role in the Marketplace.

- An agent or broker and any third party they have entered into a business relationship with must adhere to requirements for the use and disclosure of all consumer PII/protected health information (PHI), including all PII/PHI collected by the third party.
The record of the consent should include the following:

- The individual’s, employer’s, or employee’s name,
- The date the consent was given, and
- The name of the agent(s), broker(s), or agency 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.

This consent should also indicate that the agent or broker has permission to:

- Conduct a search for the consumer application using approved Classic DE/EDE websites in the Marketplace;
- Assist with completing an eligibility application;
- Assist with plan selection and enrollment; and
- Assist with ongoing account/enrollment maintenance.
Expiration of Consumer Consent

» CMS does not specify an automatic expiration date for the consent because it could become burdensome for anyone consistently seeking services from the same agent/broker or agency to have to repeatedly renew the consent.

» Therefore, the consent may last indefinitely, unless the individual, employer, or employee revokes it. As a best practice, if you are ever unsure of whether a client has decided to work with you, you should contact the client. Additionally, you may obtain consent electronically (such as via email or text message) or in person.

» Consent documents must be appropriately secured and retained for 10 years.

» The consent should acknowledge that the agent or broker has informed the consumer of the functions and responsibilities that apply to the agent’s or broker’s role in the Marketplace.

» If agents or brokers sell or transfer their book of business to another producer, they should inform consumers impacted by the sale and change of NPN. Before working with any new clients, the new agent or broker is required to obtain consumer consent.
What is Information Security?

**Information security** refers to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- Confidentiality
- Integrity
- Availability

A risk is the cost to business should a vulnerability be exploited by a threat, causing harm to an asset.

- All information systems have some level of risk.

Information system security risks are usually qualitative, typically High, Moderate, Low; and relate to the confidentiality, integrity, and availability of the information and the information system.

<table>
<thead>
<tr>
<th>Impact Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Limited adverse effect: almost no impact, with little cost, to minimal effort to repair</td>
</tr>
<tr>
<td>Moderate</td>
<td>Serious adverse effect: some tangible harm, with moderate expenditure to repair</td>
</tr>
<tr>
<td>High</td>
<td>Severe or catastrophic adverse effect: damage to reputation, loss of confidence, legal liability, considerable or extended disruption, compromise of information, full compromise of services</td>
</tr>
</tbody>
</table>
Security & Privacy

**Security** refers to the systems and physical safeguards in place to protect a consumer’s personal information.

**Privacy** is the consumer’s right to control how their personal information is used or disclosed.

<table>
<thead>
<tr>
<th>Security</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountable to management</td>
<td>Accountable to the person</td>
</tr>
<tr>
<td>Risk-based assessment.</td>
<td>Capabilities-based assessment. Is it possible?</td>
</tr>
<tr>
<td>How likely is it?</td>
<td></td>
</tr>
<tr>
<td>Access and use controls</td>
<td>Access and use controls</td>
</tr>
<tr>
<td>defined by the system</td>
<td>defined by use limitation,</td>
</tr>
<tr>
<td>owner.</td>
<td>consent of subject, and</td>
</tr>
<tr>
<td></td>
<td>legislation.</td>
</tr>
<tr>
<td>Focused on protecting</td>
<td>Protecting against</td>
</tr>
<tr>
<td>against outsiders.</td>
<td>outsiders, insiders and</td>
</tr>
<tr>
<td></td>
<td>system owner.</td>
</tr>
<tr>
<td>Encryption helps. When</td>
<td>Who has the keys? When</td>
</tr>
<tr>
<td>is it decrypted?</td>
<td>is it decrypted?</td>
</tr>
</tbody>
</table>
 Protecting Consumers’ PII

» The Marketplace Privacy and Security Agreement that you execute as part of the annual registration process authorizes agents and brokers to create, collect, disclose, access, maintain, store, and use specific data and PII. **Agents and brokers cannot release, publish, or disclose consumer PII to unauthorized personnel, and must protect this information in accordance with federal laws and regulations regarding the handling of PII.**

» PII refers to 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 which is linked or linkable to a specific individual.¹

» You must provide consumers the opportunity to opt-in and allow you (and your agency, if applicable) to use their PII (e.g., through the record of consent). You should also provide a mechanism through which the consumer, or their authorized representative, can limit the use of their PII.

¹This definition of PII was taken from the CMS.gov Privacy Policy available at [https://www.cms.gov/privacy](https://www.cms.gov/privacy).
There are many types of PII. PII is any information your organization classifies as sensitive, such as:

- Applicant address
- Applicant maximum APTC amount
- Applicant CSRs level
- Applicant household income
- FFE applicant ID
- Checking account and routing number

Other types of protected information include:

- Private health information (PHI), such as medical histories and lab results
- Federal Tax Information
How to Protect Consumers’ PII

As an agent or broker, you can protect consumers’ PII by:

- Applying a “need to know” principle before disclosing PII to other personnel
- Evaluating a requested need for PII before sharing others
- Limiting PII to official use only

Agents and brokers are also required to train and monitor their staff on the requirements related to the authorized use and sharing of PII with third parties and the consequences of unauthorized use or sharing of PII, and periodically audit their actual use and disclosure of PII.

¹ This information was taken from the Individual Marketplace Privacy and Security Agreement for Plan Year 2022, Section II, Paragraph E “Duty to Protect PII.”
Kelly is working on a client report for her manager. It is faster for Kelly to pull existing client data from another report than create a new one. The existing report also contains social security numbers and birthdates, information Kelly does not need. Is it okay for Kelly to use the report to save time?

a) Yes, because it will help her do her job.
b) No, agents and brokers should only access information as needed to perform their job function and for authorized purposes only.
Best Practices for Protecting PII

**In Person**
- Secure hard-copy consumer consent forms in a locked location.
- During consumer appointments, utilize private spaces to ensure privacy.
- Dispose of PII in a manner consistent with FFM rules and retention requirements.

**Electronic**
- Do not send or forward emails with PII to personal email accounts.
- Do not use unauthorized mobile devices to access PII.
- Store PII securely in a password-protected file on a password-protected computer to which only authorized individuals have access.

**Paper**
- Ensure any originals of consumers' records are returned before they leave your office and only make copies for yourself or others if necessary to carry out required duties.
- Keep a supply of manila folders to give to consumers with their documents inside to keep them in one place and shield the contents from view.
Knowledge Check #2

What does it mean to protect PII by limiting authorized use and sharing of PII with third parties?

a) Agents and brokers must apply a need-to-know principle when it comes to authorized use of PII, and if agents or brokers sell or transfer their book of business to another producer, they should inform consumers impacted by the sale and change of NPN.

b) Agents and brokers should not share PII with anyone else under any circumstances.

c) Agents and brokers can share PII with anyone in their organization, as long as the PII is not shared with anyone outside of the organization.

d) Agents and brokers cannot share PII with anyone in their organization, even if it means helping the consumer with necessary enrollment functions.
Suspension for Risk to Marketplace Operations or Systems

CMS may immediately suspend an agent’s or broker’s ability to access Marketplace systems if it discovers circumstances that pose unacceptable risk to Marketplace operations or information technology systems until the incident or breach is remedied or sufficiently mitigated to HHS' satisfaction.

- Applying this provision would suspend an agent’s or broker’s access to the CMS Enterprise Portal, the Marketplace Learning Management System (MLMS), and the Classic DE/EDE Pathways.
- Termination under 45 C.F.R. § 155.220(g)(5) will include 30-days’ advance notice, in which agents have the opportunity to submit evidence to rebut CMS’ conclusions prior to the termination.

If your Marketplace access is ever suspended and you have questions about your suspension, please contact the Agent/Broker Help Desk: FFMProducer-AssisterHelpDesk@cms.hhs.gov
Cybersecurity Breaches

» Cybersecurity breaches are a growing threat for small businesses.

» Small businesses are targeted because they have information that hackers want, and they often lack the security infrastructure of larger businesses.

» 88% of small business owners felt their business was vulnerable to a cyber-attack, according to a recent Small Business Administration survey. Yet many businesses don’t know where to begin when it comes to cybersecurity.
Breaches vs. Incidents

» A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for anything other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.¹

Some common examples of breaches include:
  » A laptop or portable storage device storing PII is lost or stolen;
  » An email or letter containing PII is inadvertently sent to the wrong person; and
  » An authorized user accesses or uses PII for an other-than-authorized purpose.

» An incident is an adverse event or action that is unplanned, unusual, and unwanted that happened as a result of non-compliance with the privacy policies and procedures of the organization. It must pertain to the unauthorized use or disclosure of PII including “accidental disclosure” such as misdirected e-mails or faxes.¹

¹These definitions are taken from the Office of Management and Budget (OMB) Memorandum 17-12 available at https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf.
Types of Breaches and Incidents

A security incident is a reportable event that meets one or more of the following criteria:

- The successful unauthorized access, use, disclosure, modification, or destruction of information or interference with operations in an information system.
- The loss of data through theft, device misplacement, misplacement of hardcopy documents, and misrouting of email.
- An occurrence that actually or potentially jeopardizes the confidentiality, integrity, and availability of an information system or the information.
- A violation or threat of violation of computer security policies, acceptable use policies, or standard security practices.

Common threats include:

- Social engineering
- Phishing
- Malware (Viruses, ransomware, etc.)
- Inadequate or delayed patching
Examples of PII Incidents

- Theft of a laptop, thumb drive or portable hard drive containing encrypted or unencrypted PII.
- Mailing hard-copy documents containing PII to the incorrect address.
- Unauthorized access to personnel or medical files.
- Email containing medical information transmitted from business email account to a personal email account.
- A hacker gains access to a computer and its accounts.
- Leaving documents containing PII exposed in an area where individuals without approved access could read, copy, or move it for future use.
Common Threats: Social Engineering

» “Social engineering” attempts to manipulate you into unwittingly divulging information to a hacker, or into taking an action that leads to a security or privacy breach.

» Hackers could appear to be a coworker or a “friend” in an effort to gain your trust so they can obtain access to your information and information systems.

» Hackers can also lurk in free Wi-Fi networks, such as those at coffee shops, airports, and hotels.

Social engineering looks like:

» Normal appearing websites that seem to be legitimate may be compromised with malicious links or malware infecting visiting devices.

» “Friend requests” on social networks may impersonate friends and colleagues to trick you into accepting malware or divulging sensitive information.
Common Threats: Phishing

Phishing is a form of social engineering whereby intruders seek to gain access to information and information systems by posing as a real person, business or organization with legitimate reason to request the information.

Phishing emails (or texts) often alert the user to a problem with their account and ask the user to click on a link to provide information to correct the problem.

These links can download malicious programs onto your computer or mobile device and allow the attacker access to the device, connected devices, and the information stored on those devices.

These emails often look real and appear to contain real organizational logos and trademarks. They may be personally addressed to you and appear to be sent from a legitimate source you know and trust, like a government agency or professional organization.

The URL provided may even resemble the authentic URL web address, for example, “Amazons.com” with a very minor spelling error that one could easily overlook.

Phishing vs. Spear Phishing vs. Whaling

- **Phishing**
  A broader term that covers any type of attack that tries to fool a victim into taking some action. Does not have a specific target.

- **Spear Phishing**
  A type of phishing that targets individuals.

- **Whaling**
  A form of spear phishing that targets high-ranking victims within a company.
Common Threats: Malware

Malware (short for malicious software) does damage to, steals information from, or disrupts a computer system.

Malware is commonly installed through a user:
- Opening infected email attachments.
- Downloading infected files.
- Visiting an infected website.

Malware (to include ransomware) can corrupt files, erase your hard drive, or give a hacker control of your computer.

Protect yourself from malware by:
- Reading emails in plain text.
- Scanning attachments with antivirus software before downloading. Never open an attachment from someone you do not know.
- Using the Spam button to report suspicious emails without opening them.

If you believe your business computer containing Marketplace sensitive information is infected, contact the CMS IT Help Desk at CMS_IT_Service_Desk@cms.hhs.gov.
Common Threats: Ransomware

» Ransomware is a type of malware that infects and restricts access to a computer, encrypting files and rendering them and the systems that rely on them unusable.
» Hackers then demand to be paid ransom in exchange for decryption.

Ransomware looks like:
» Phishing emails.
» Exploiting unpatched vulnerabilities in software.
Agents and brokers should follow precautionary “cybersecurity hygiene” measures to keep sensitive client data secure and protect it from theft and attacks.

Cybersecurity hygiene is a set of practices that should be performed regularly to maintain the security of devices and networks.

What can you do?
- Learn more about common cyber threats.
- Understand where your business is vulnerable.
- Take steps to improve your cybersecurity.

Cybersecurity hygiene practices include:
- **Backup**: Regularly back up important files to a separate, secure location that would remain safe in case of a cybersecurity breach.
- **Awareness & Education**: Learn how to avoid phishing scams and how to prevent malware attacks. Agents and brokers should also share this information with their employees.
- **Encryption**: Use encryption to protect sensitive data in files and on devices.
Cybersecurity hygiene best practices also include:

- **Password hygiene**: Maintain good password hygiene by requiring unique passwords, employing password managers, reviewing cycle frequency, and using multifactor authentication (MFA) when possible to make it more challenging for hackers to gain unauthorized access.

- **Patch management**: Always keep software up to date and install security patches on both company-owned devices and personal devices used for work.

- **Security software**: Install security software to defend systems against malware such as ransomware, spyware, worms, rootkits and Trojans. Also, run regular scans to flag unusual activity.
Dan has received an email that is personally addressed to him and appears to be sent from a legitimate source that he knows and trusts. The email notifies him that there is a problem with his account and asks him to click a link to provide information to correct the problem. Dan was not aware of a problem with his account and is hesitant about clicking the link. He also notices that the URL provided resembles an authentic web address, but has a very minor spelling error, for example, “Googlle.com.” What should he do? Select all that apply.

- a) Click the link and provide information to correct the problem with his account.
- b) Check with his IT department to ensure the email is legitimate.
- c) Do not click on the email and delete the message.
- d) Forward the email to his colleague and ask them if the email is legitimate.
Taylor is traveling and the hotel she is staying at offers free Wi-Fi. Is it okay for her to use this Wi-Fi to access her business email and protected business files?

a) No, connecting to free, unsecure Wi-Fi networks can expose her computer to unnecessary security risks.

b) Yes, the hotel wouldn’t offer free Wi-Fi if it wasn’t safe to use.

c) Yes, she will only connect to the Wi-Fi for a short amount of time.
Preventing Cybersecurity Breaches

Agents and brokers should follow these steps to prevent cybersecurity breaches:

1. Review the information provided in this webinar and other CMS privacy and security resources.
2. Identify the types of information your business will access, process, store, or transmit.
3. Identify user access, password strength, and security procedures for all systems.
4. After assessing potential risks, establish boundaries that will protect PII and other sensitive information.
5. Implement appropriate boundaries for your business.
Agents and brokers should follow security breach and incident response phases and document each step toward resolution:

- **Identification:** Identify the incident
- **Preparation:** Prepare information to report
- **Response:** Report to the CMS IT Help Desk
- **Recovery:** Work to rebuild security systems
- **Follow-up:** Work with CMS to resolve the issue

**Knowing how to respond during an incident:**
- Helps resolve the issue efficiently.
- Minimize loss of information.
- Minimize disruption of services or breach of security.
Reporting Cybersecurity Breaches

When in doubt– Report!

» All potential and confirmed breaches and incidents must be reported to CMS. If you’re unsure whether the situation is a breach, an incident, or nothing at all, it is better to report it.
» Don’t wait until you have finished internal investigations to report a breach or incident.
» We take “good faith” efforts to report an incident timely into account, but the reporting timelines are in place to ensure consumer safety.

» The Agent Broker Individual Marketplace Privacy and Security Agreement and Agent Broker SHOP Agreement requires the following:
  o Require reporting any Breach of PII 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 24 hours from knowledge of the Breach. Incidents must be reported to the CMS IT Service Desk by the same means as Breaches within 72 hours from knowledge of the Incident. Reporting a breach or incident is not an admission of wrongdoing.

» If you are an agent or broker who uses the DE or EDE partner sites for your enrollments, and you believe someone else has used or accessed your account, you must immediately report the incident to the CMS IT Service Desk and the DE/EDE partner website’s Agent Broker Help Desk. Please also make sure that you update your passwords to login to your DE/EDE account as soon as possible.
Remediation of Cybersecurity Incidents

When contacting the CMS IT Service Desk via email regarding a security breach or incident, it is best practice to submit a Security Incident Report (SIR). The SIR template can be found at:


After you report:

- The Incident Management Team (IMT) will issue an incident number for tracking.
- IMT will escalate to the appropriate teams that are responsible for tracking and investigation.
- If you have additional information to provide regarding your incident report, you can provide updates by calling or emailing the CMS IT Service Desk. Please state that you are providing an update and use the incident number that was issued when you originally reported.
The CMS Information Security and Privacy Library is a resource to provide additional information about how CMS conducts cybersecurity.

CISA’s Cyber Essentials serves as a guide for small businesses to develop an understanding of where to start implementing cybersecurity practices.

The Small Business Administration offers free training sessions on cybersecurity. Sign up for their trainings here.

The National Cybersecurity Alliance also provides virtual and in-person cybersecurity events to help small business owners learn about cybersecurity and how to stay secure.

For more information on compliance in the Marketplace, see the Compliance with Marketplace Requirements: Reminders for Agents and Brokers webinar slides.
Knowledge Check #5

How can I identify and report a cybersecurity breach?

a) By waiting until you are sure it is a cybersecurity breach and then calling the police.

b) By trying to resolve the issue yourself and not reporting it.

c) By trying to resolve the issue yourself, and if you are not able to, contacting the CMS IT Service Desk.

d) By teaching yourself to identify cybersecurity breaches and contacting the CMS IT Service Desk within 24 hours if one should occur.
Knowledge Check #6

How can I maintain a level of security that is consistent with CMS compliance requirements and will offer the most protection to my clients and business?

a) By reviewing the CMS Privacy and Security Agreement and the 2022 Agent Broker Agreement to ensure compliance and to implement the appropriate security controls.

b) By reviewing the CMS Privacy and Security Agreement and the 2022 Agent Broker Agreement and then implementing maximum security controls on all devices.

c) By finding another online training on cybersecurity and using those requirements to update system controls and devices.

d) By asking all clients which level of security they are most comfortable with.
Knowledge Check #7

Why is it important to only access the minimal amount of resources and information required to perform enrollment functions?

a) Because access to sensitive information should be available to everyone.
b) Because access to sensitive information should only be granted for necessary enrollment functions.
c) Because access to sensitive information should be available to no one except the agent or broker working with the consumer.
d) Because access to sensitive information should only be granted to people in your organization.
# Agent/Broker Marketplace Help Desks and Call Centers

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone # and/or Email Address</th>
<th>Types of Inquiries Handled</th>
<th>Hours (Closed Holidays)</th>
</tr>
</thead>
</table>
| Marketplace Service Desk          | 1-855-CMS-1515               | - CMS Enterprise Portal password resets and account lockouts  
- Other CMS Enterprise Portal account issues or error messages  
- General registration and training questions (not related to a specific training platform)  
- Login issues on the DE agent/broker landing page  
- Technical or system-specific issues related to the MLMS  
- User-specific questions about maneuvering in the MLMS site, or accessing training and exams |
|                                   | 1-855-267-1515               | Monday–Friday 8:00 AM–8:00 PM ET  
October–November only: Saturday–Sunday 10:00 AM–3:00 PM ET |
| 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 RCL issues  
- Find Local Help listing issues  
- Help On Demand participation instructions or questions  
- Report concerns that a consumer or another agent or broker has engaged in fraud or abusive conduct |
|                                   |                              | Monday–Friday 8:00 AM–6:00 PM ET |
| Marketplace Call Center           | 1-855-788-6275               | Specific consumer application questions related to:  
- Password reset for a consumer HealthCare.gov account  
- SEP not available on the consumer application, or  
- Consumer specific eligibility and enrollment questions |
| Agent/Broker Partner Line         | Note: Enter your NPN to access this line. TTY users 1-855-889-4325 | Monday–Sunday 24 hours/day |
| CMS IT Service Desk               | (410) 786-2580 or 1-800-562-1963 CMS_IT_Service_Desk@cms.hhs.gov | - Reporting a security breach or incident |
|                                   |                              | Monday–Friday 9:00 AM–5:00 PM ET |

A full list of Agent/Broker Help Desks and Call Centers is available from the Agent and Broker Resources webpage (http://go.cms.gov/CCIIOAB) under Quick Links.
## Acronym Definitions

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCIIO</td>
<td>Center for Consumer Information and Insurance Oversight</td>
</tr>
<tr>
<td>CMS</td>
<td>Centers for Medicare &amp; Medicaid Services</td>
</tr>
<tr>
<td>DE</td>
<td>Direct Enrollment</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>EDE</td>
<td>Enhanced Direct Enrollment</td>
</tr>
<tr>
<td>FTI</td>
<td>Federal Tax Information</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>HITECH</td>
<td>Health Information Technology for Economic Clinical Health Act</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMT</td>
<td>Incident Management Team</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>PHI</td>
<td>Protected Health Information</td>
</tr>
<tr>
<td>PPACA/ACA</td>
<td>Patient Protection and Affordable Care Act</td>
</tr>
<tr>
<td>SIR</td>
<td>Security Incident Report</td>
</tr>
<tr>
<td>SSN</td>
<td>Social Security Number</td>
</tr>
</tbody>
</table>
Agents and brokers are valued partners to all of us at CMS for the vital role you play in enrolling consumers in qualified health plan coverage offered through the Marketplace.

We thank you for the trusted advice, support, and assistance you provide throughout the year and wish you continued success!