
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

The Marketplace and Cybersecurity

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

February 2024

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Topics

01 Common Threats Against Personally Identifiable Information (PII)

02 Information Security and PII

03 Cybersecurity Threats and Incidents

04 Cybersecurity Hygiene

05 Cybersecurity Resources

Common Threats Against PII

- Protecting the PII of your clients is one of your most important roles as an agent or broker. A crucial part of protection is prevention – being aware of cyber threats that can come from a text, email, or anywhere else online.
- Keep the statistics below in mind as you think about how cyber threats can affect you, and how to talk about them with your clients.

Types of PII

- PII is information which can be used alone, or in combination with other data elements, to distinguish or trace an individual's identity.
- To effectively handle PII, consult this frequently asked question (FAQ) to learn about requirements for agents and brokers.
- There are many types of PII, which can include:
  - Applicant address;
  - Applicant maximum advance payment of the premium tax credit (APTC) amount;
  - Applicant cost-sharing reductions (CSRs) level;
  - Applicant household income;
  - Federally-facilitated Exchange (FFE) applicant identification (ID);
  - Checking account and routing number;
  - Private health information (PHI), such as medical histories and lab results;
  - Federal Tax Information.

Protecting Consumers' 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.
- 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.
  - Please consult the Individual Marketplace Privacy and Security Agreement for Plan Year 2024, Section II, Paragraph E "Duty to Protect PII" for further information on working with consumer PII.

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.
- **Online**
  - Do not send or forward emails with PII to personal accounts.
  - Do not use unauthorized mobile devices to access PII.
- **When working with others**
  - 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.

PII Incident Scenario

CMS' cybersecurity expert, Charlie, asks…

Jackson was sifting through a document containing PII, where several Social Security numbers (SSNs) were displayed. He copies his supervisor on an email to gather his thoughts on an approach with regards to this information but forgets to encrypt the email with a password. Why do Jackson's actions indicate a potential breach of PII?

PII Incident Scenario (continued)

» Jackson's actions indicate a potential breach of PII because if he copies sensitive information on an email without encryption (such as password protecting it) this therefore leaves the information vulnerable to outside parties such as hackers. SSNs constitute PII.

Tip from CMS' cybersecurity expert, Charlie:

If PII must be sent over email, it needs to be encrypted and follow certain protocols to protect the data.

Knowledge Check #1

CMS' cybersecurity expert, Charlie, asks…

Fatimah is working on a client report for her manager. It is faster for Fatimah to pull existing client data from another report than create a new one. The existing report also contains SSNs and birthdates, information Fatimah does not need. Is it okay for Fatimah to use the report to save time?

a) Yes. It will help her do her job.

b) No. As an agent or broker, Fatimah should only access information as needed to perform her job function and for authorized purposes only.

Knowledge Check #1: Answer

CMS' cybersecurity expert, Charlie, asks…

Fatimah is working on a client report for her manager. It is faster for Fatimah to pull existing client data from another report than create a new one. The existing report also contains SSNs and birthdates, information Fatimah does not need. Is it okay for Fatimah to use the report to save time?

a) Yes, because it will help her do her job.

b) No – as an agent or broker, Fatimah should only access information as needed to perform her job function and for authorized purposes only.

Knowledge Check #2

CMS' cybersecurity expert, Charlie, asks…

> What are the restrictions for agents and brokers sharing PII?

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 national producer number (NPN).

b) 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.

c) Agents and brokers cannot share PII with anyone in their organization, even if it means helping the consumer with necessary enrollment functions.

Knowledge Check #2: Answer

CMS' cybersecurity expert, Charlie, asks…

> What are the restrictions for agents and brokers sharing PII?

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 can share PII with anyone in their organization, as long as the PII is not shared with anyone outside of the organization.

c) 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 the Department of Health and Human Services' (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 Direct Enrollment and Enhanced Direct Enrollment (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

Accessing CMS Systems Abroad

- Agents and brokers may not access CMS systems at any point if they are outside of the United States of America (U.S.) or U.S. Territories. This includes DE and EDE partner websites.
- If a consumer is submitting or updating their application on HealthCare.gov and the consumer contacts the agent or broker while the agent or broker is outside of the U.S., it is possible for the agent or broker to provide verbal or written assistance to the consumer.
  - Note: Agents and brokers may never create a HealthCare.gov account for a consumer or log into a consumer's HealthCare.gov account—whether in the U.S. or outside of the country.
- As stated in the Agent Broker Agreements, agents and brokers are not allowed to remotely connect or transmit data to the FFE, state-based exchange on the federal platform (SBE-FP), or its testing environments nor remotely connect from locations outside of the U.S. or its territories, embassies, or military installations. This includes any such connection through VPNs.

Accessing CMS Systems Abroad (continued)

- Examples of systems and websites that agents and brokers may not access from outside of the U.S. include:
  - HealthCare.gov and private DE and EDE websites.
  - The CMS Enterprise Portal.
  - The REGTAP library. Note: Recordings and slide decks from REGTAP-hosted webinars and events are posted online and are available for review at any point. To access CMS slide decks, visit the General Resources page.
- Additionally, agents and brokers may not use professional or IT services, call center/customer support operations, or software tools that are not located or hosted in the U.S. or one of its territories, embassies, or military installations.
- If you need additional assistance or to report suspected violations of these Marketplace requirements, contact the Agent/Broker Email Help Desk at FFMProducer-AssisterHelpDesk@cms.hhs.gov.

Cybersecurity Incidents

- 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]
- 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.

[1]These 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.

Cybersecurity Incidents (continued)

- Common threats include:
  - Social engineering;
  - Phishing;
  - Malware (Viruses, ransomware, etc.);
  - Inadequate or delayed patching.

Common Threats: Social Engineering

- **Definition:** 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" 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.
- **Examples:**
  - 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: Social Engineering (continued)

- **Prevention:**
  - Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
  - Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
  - Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.

Common Threats: Phishing

- **Definition:** 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.

- **Examples:**
  - 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.

Common Threats: Phishing (continued)

- **Prevention:**
  - Maintaining current anti-virus software.
  - Regularly updating the software on your computer and cell phone.
  - Utilizing a multi-factor authentication (MFA) with all your accounts.
  - Backing up the data on your computer and cell phone.
  - Filtering spam emails.
  - Not clicking links or opening attachments.
- If you become aware of a breach or incident involving PII as a result of phishing, report this situation immediately to the appropriate organization. In addition, change the password to any account that may be compromised.
- You can also report the cyberattack to the police, file a report with the Federal Trade Commission, or report the cyberattack to the Federal Bureau of Investigation (FBI), the lead federal agency for investigating cyberattacks and intrusions.
- For further information on phishing, check out this tip sheet.

Common Threats: Malware

- **Definition:** Short for malicious software, malware does damage to, steals information from, or disrupts a computer system. It is commonly installed through a user:
  - Opening infected email attachments.
  - Downloading infected files.
  - Visiting an infected website.
- **Examples:** Examples of malware include:
  - Viruses;
  - Worms;
  - Trojans;
  - Ransomware;
  - Spyware;
  - Rootkits.

Common Threats: Malware (continued)

- **Prevention:**
  - 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

- **Definition:** 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.
- **Examples:**
  - Phishing emails.
  - Exploiting unpatched vulnerabilities in software.
- **Prevention:**
  - Never click on unverified links.
  - Scan emails for malware.
  - Only download from trusted sites.
  - Keep backups of important data.
  - Use a virtual private network (VPN) when using public Wi-Fi.

Knowledge Check #3

CMS' cybersecurity expert, Charlie, asks…

Dan received an email that is personally addressed to him and appears to be sent from a legitimate source that he trusts. The email notifies him that there is a problem with his account and asks him to correct it. Dan is hesitant about clicking the link. He also notices that the URL provided resembles an authentic web address but contains a spelling error. 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.

Knowledge Check #3: Answer

CMS' cybersecurity expert, Charlie, asks…

Dan received an email that is personally addressed to him and appears to be sent from a legitimate source that he trusts. The email notifies him that there is a problem with his account and asks him to correct it. Dan is hesitant about clicking the link. He also notices that the URL provided resembles an authentic web address but contains a spelling error. 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.

Knowledge Check #4

CMS' cybersecurity expert, Charlie, asks…

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.

Knowledge Check #4: Answer

CMS' cybersecurity expert, Charlie, asks…

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.

Cybersecurity Breaches

- 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 PII, whether physical or electronic.
- 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.

Some common examples of breaches include:

Preventing Cybersecurity Breaches

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

1. Identify the types of information your business will access, process, store, or transmit.

2. Identify user access, password strength, and security procedures for all systems.

3. After assessing potential risks, establish boundaries that will protect PII and other sensitive information.

4. Implement appropriate boundaries for your business.

Responding to Breaches and Incidents

- Agents and brokers should follow security breach and incident response phases and document each step toward resolution:

- 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 Small Business Health Options Program (SHOP) Agreement requires the following:
  - 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 change your passwords to login to your CMS Enterprise Portal and 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:
  - https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response-Appendix-K-Incident-Report-Template
- 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.

Practicing Cybersecurity Hygiene

- 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:

Practicing Cybersecurity Hygiene (continued)

- Cybersecurity hygiene best practices also include:
  - **Password hygiene:** Maintain good password hygiene by requiring unique passwords, employing password managers, reviewing password change cycle frequency, and using 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.
  - For more information on cybersecurity hygiene, view this tip sheet.

Practicing Cybersecurity Hygiene: Encryption

- Encryption is essential because it adds an extra layer of security to PII. You can assure your clients that you are protecting their information and that their files and data will be securely stored on your device. This can be done by:
  - Being aware of what information is stored on your devices and who has access to it.
  - Deleting any unnecessary PII from your devices.
  - Encrypting PII that is kept on your devices or sent via email, over a wireless network, or through the
  - internet.
  - Using encryption when remote access is used on your device (e.g., if a company troubleshoots your software remotely).
  - Overwriting the data so unauthorized individuals won't be able to access the information.

Practicing Cybersecurity Hygiene: Encryption (continued)

- Encryption best practices:
  - If you are the owner of an agency, train your employees on how to properly encrypt sensitive data on their devices.
  - Ensure you know how to encrypt the data on your devices.
  - Ensure the encryption is configured correctly. If it isn't, the information will not be protected.
  - Have a plan in mind if encryption fails or PII is leaked.
- For more information on encryption, see this tip sheet.

Anti-Virus Software

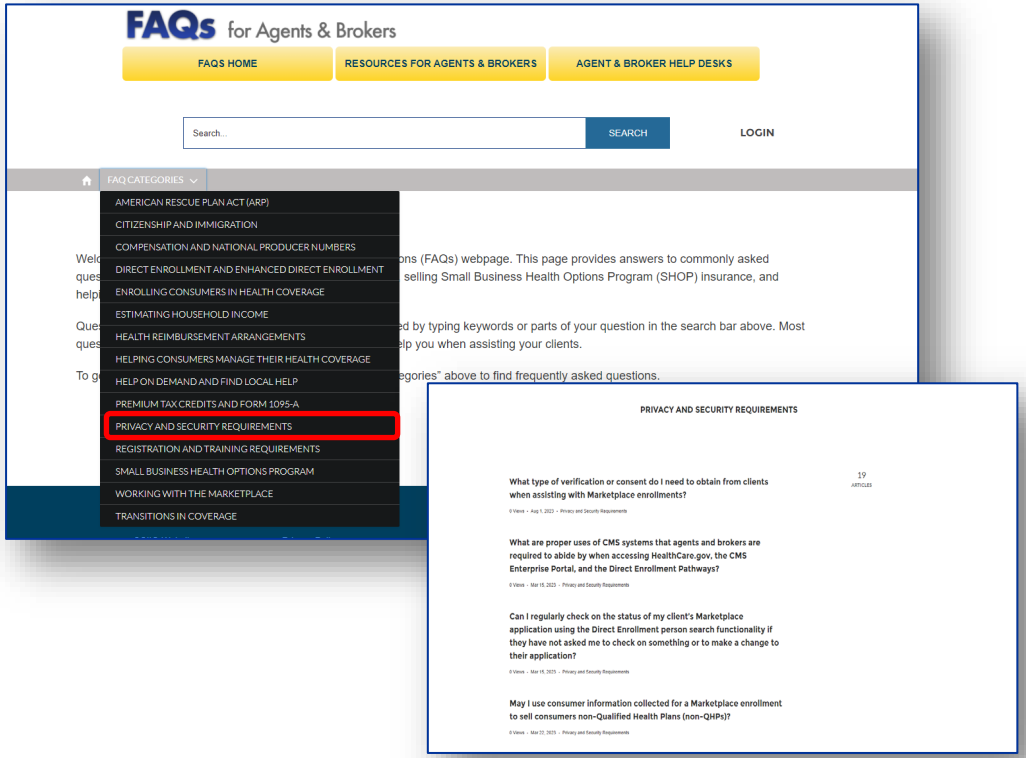
- **Anti-virus software** scans files or your computer's memory for certain patterns that may indicate the presence of malicious software (i.e., malware). Anti-virus software (sometimes more broadly referred to as anti-malware software) looks for patterns based on the signatures or definitions of known malware.
  - It is considered a best practice to install an antivirus program on your computer that will conduct automatic updates. Programs with automatic updates usually come with a suite of tools including a VPN service. However, even implementing a tool that is generally available through your computer company would be better than not having any kind of antivirus program. See this guidance from the Cybersecurity & Infrastructure Security Agency (CISA) on understanding antivirus software.
  - If you need additional assistance on this topic, contact the Agent/Broker Email Help Desk at FFMProducer-AssisterHelpDesk@cms.hhs.gov.

Anti-Virus Software (continued)

- **How will the software respond when it finds malware?**
  - Sometimes the software will produce a dialog box alerting you that it has found malware and ask whether you want it to "clean" the file (to remove the malware). In other cases, the software may attempt to remove the malware without asking you first. When you select an anti-virus package, familiarize yourself with its features so you know what to expect.
- **Which software should you use?**
  - There are many vendors who produce anti-virus software, and deciding which one to choose can be confusing. Anti-virus software typically performs the same types of functions, so your decision may be driven by recommendations, particular features, availability, or price. Regardless of which package you choose, installing any anti-virus software will increase your level of protection.

Privacy and Security Requirements FAQs

- The Agent and Broker FAQs website includes a category dedicated to Privacy and Security FAQs.
  - Note: This FAQs page has been updated to include Consumer Consent and Application Review Requirement FAQs.
- This self-service resource is available online and is linked in the Agent and Broker Resources webpage.



Resources on Cybersecurity

- The CMS Information Security and Privacy Group (ISPG) website provides 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 Federal Trade Commission has a list of videos on topics such as cybersecurity basics, ransomware, and more. Click here to access these videos and view additional cybersecurity content for small businesses.
- 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 maintaining compliance in the Marketplace, see the Marketplace Compliance webinar slides and the Agent/Broker Summit: Marketplace Compliance and Agent/Broker Regulations webinar slides.