Course 4 Privacy, Security, and Fraud Prevention Standards

Module 1 – Privacy, Security, and Fraud Prevention Standards

Course Introduction

Privacy, Security, and Fraud Prevention Standards

Welcome

I’m Neha and I’ll be helping you learn the answers to these questions and more as we cover the topics of privacy, security, and fraud prevention in this course.

- Are you permitted to ask consumers for their Social Security Numbers (SSNs) or their driver's license numbers?
- What would happen if you or your office manager mix up two consumers by accidentally sending an email containing one consumer's name, date of birth, and address to the other?

Course Goal

This course will help you understand the privacy and security standards applicable to the Federally-facilitated Marketplace (FFM or Marketplace) and will explain how to recognize and prevent fraud. Obtaining consumers' consent to access and use their personally identifiable information (PII) is a mandatory requirement before you access and use consumers' information in your role as an assister.

Goal:

This course will help you understand the importance of privacy and security in handling consumers' PII. You'll learn potential risks, best practices for preventing these risks, and best practices for handling data breaches.

Topics:

By the end of this course, you'll understand:

- Examples of PII.
- Marketplace privacy requirements.
- Consumer consent.
- Restrictions on use of PII.
- Protecting PII.
- Privacy, security, and confidentiality.
- Privacy and security incidents and breaches.
- Information security.
- Fraud in the Marketplaces.
- Preventing fraud.
- Reporting fraud.

Module 2 - Protecting Consumer Information

Introduction

By the end of this module, you'll understand the following concepts and be able to accomplish the tasks below them.

Examples of Personally Identifiable Information (PII)

List examples of PII and how this information is used by the Federally-facilitated Marketplace (FFM).

Marketplace Privacy Requirements

List steps you must take to comply with Marketplace privacy requirements.

Consumer Consent

Describe information in the Privacy Notice Statement, your organization's consent form (if applicable), and ways to obtain consumer consent.

Restrictions on PII

Understand and adhere to restrictions on the use of consumer PII.

Protecting PII

Describe techniques and best practices to protect PII.

Key Terms

Define the terms privacy, security, and confidentiality.

PII Definition

Before we get started, let’s discuss how to identify PII.

PII is information that can be used to distinguish or trace a consumer's identity, either alone or combined with other personal or identifiable information that is linked or linkable to a specific individual.

Common examples of PII include:

- Name.
- Social Security Number (SSN).
- Date and place of birth.
- Mother’s maiden name.
- Medical, educational, financial, and/or employment information.
- Phone number.
- Home address.
- Driver’s license number.
- Electronic or paper tax returns (e.g., 1040, 1099, 1120, and W-2).

When You'll Come in Contact With PII

You'll likely collect, disclose, access, maintain, store, and/or use consumers' PII each time you'll help them:

- Create a Marketplace account.
- Complete the eligibility process and submit an application for coverage.
- Assess options for lowering costs of coverage.
- Enroll in a qualified health plan (QHP).

Key Privacy Requirements for Assisters

Before you begin helping consumers, there are some important things you must do to follow Marketplace privacy requirements:

- Make sure your organization has appropriate written policies and procedures for collecting, protecting, and securing all PII.
- Provide consumers with a Privacy Notice Statement before you collect PII or other information from them. If your organization uses a paper or electronic form to gather or request PII from consumers, this statement may be included on that form.
- Clearly display the Privacy Notice Statement on your organization's public-facing website if you use such a website to collect PII or other consumer information.
- Always obtain consumers' consent, or "authorization," before collecting or accessing their personal information.
- Let consumers know what personal information you'll collect, why it's collected, how you'll use it, with whom the information can be shared, and what happens if they don't want to provide it.
- Only collect information that is necessary to assist consumers unless they give you specific consent for additional uses.

All these requirements are included in the privacy and security requirements your organization received when it was approved to help consumers. You must be familiar with these requirements to make sure consumers' privacy is protected. Keep in mind that sub-grantees, or organizations you'll contract with, must be held to the same standards regarding the use and disclosure of consumers' PII.

Key Privacy Requirements for Assisters (Cont'd.)

Consumers might ask why you'll need to discuss so much personal information with them when you help them apply for and enroll in coverage through the Marketplaces. You should inform them that the Marketplaces use their PII to:

- Determine or assess eligibility for Marketplace coverage, Medicaid, and Children's Health Insurance Program (CHIP) coverage.
- Determine eligibility for programs to lower costs of coverage.
- Display QHP options.
- Process eligibility appeals, if applicable.

You should also tell consumers that by accessing their PII you can:

- Help them make their own informed choices about which coverage option best meets their needs and budget.
- Make certain kinds of referrals to other individuals or organizations that can help them, like licensed tax advisers or legal aid programs.
- Advise consumers about other topics that fall within the scope of your authorized assister duties.

Before you begin assisting consumers, make sure they understand how you, your organization, and the Marketplace will use their PII to help them apply for and enroll in Marketplace coverage.

The Marketplace provides consumers with a Privacy Policy posted at the HealthCare.gov Privacy Policy webpage. In addition, there is a Privacy Act Statement the application filer must read and acknowledge when they start an application for Marketplace coverage.

You should also:

- Explain to consumers that the Marketplace has privacy and security standards and procedures in place to protect consumers' PII.
- Assure consumers that PII collected by the FFMs will be used only for fulfilling authorized Marketplace functions.

Key Tip

You're permitted to collect a consumer's name, mailing address, email address, and/or telephone number without first providing a written Privacy Notice Statement if you're using this information solely to:

- Follow up with the consumer and conduct an authorized assister function.
- Send educational information to the consumer that is directly relevant to your authorized assister functions.

This is discussed in more detail later in this course.

Knowledge Check

What activities are part of your authorized assister functions and would require you to ask for and obtain a consumer's PII?

Answer: You may obtain and use PII, like information about a consumer's residency or income, while performing authorized assister functions. Authorized functions might include helping a consumer obtain an assessment of the consumer's Medicaid eligibility, assisting a consumer in determining whether they qualify for programs to lower costs through an FFM, and helping a consumer enroll in a QHP through an FFM. You would not obtain PII simply by distributing materials at an outreach event, although that is an authorized assister function. Generally, you should only use consumer PII to the extent necessary to accomplish a specific purpose related to the FFM assistance you'll provide. You may use PII for another lawful purpose, but you must obtain a consumer's specific consent first.

Privacy Notice Statement

You should be familiar with two important documents that you must use to comply with privacy standards: the Privacy Notice Statement and the Record of Authorization. Depending on your organization's policies and procedures, the record of a consumer's consent might be a completed consent form.

Before you can collect PII or other information from consumers, you and/or your organization must provide a Privacy Notice Statement to them. Among other things, this statement explains what personal information is collected, why it's collected, how it will be used, with whom the information can be shared, for what purposes it can be shared, and how the information will be kept secure.

If your organization maintains a website that is used to gather or request PII or other consumer information, the Privacy Notice Statement must be prominently and clearly displayed on the organization's website.

The Privacy Notice Statement should explain how consumers can file a complaint with the Centers for Medicare & Medicaid Services (CMS) and your organization related to you and/or your organization's activities with respect to their information.

Your organization must review the Privacy Notice Statement at least annually and revise as necessary, including after any change to the organization's privacy policies and procedures.

You’re permitted to collect a consumer's name, mailing address, email address, or telephone number without first providing a written Privacy Notice Statement if you’re using this information solely to:

- Follow up with the consumer and conduct an authorized assister function, like scheduling an appointment for application assistance.
- Send the consumer educational information that is directly relevant to your authorized functions.

Consumer Authorization

Next, we'll discuss consumer authorization. The record of a consumer's consent, known as the Record of Authorization, is one of the most important documents you'll use in your work with consumers. Before you help consumers, you must discuss your roles and responsibilities with them and obtain consent to access their PII. This is sometimes called getting the consumer's authorization.

Consumer's Authorization/Consent

If you're a Certified Application Counselor (CAC), Enrollment Assistance Personnel (EAP) or Navigator in a Marketplace, there is a CMS model authorization form that you or your organization may adapt for your purposes. However, your organization is free to develop its own form or procedures if the consumer's authorization for obtaining consent includes, at a minimum:

1. Acknowledgment that the consumer received information about Navigator, EAP, and/or CAC roles and responsibilities. A list of roles and responsibilities is contained in Attachment A of the authorization forms.
2. Definitions of terms
3. Authorizations:
    a. General consent to access and use the consumer's PII to carry out your Marketplace functions and responsibilities.
    b. Specific consent(s) to obtain the consumer's PII for other purposes.
4. Additional information about the Navigator's, EAPs or CAC's use of consumer PII:
    a. Will ask the consumer only for the minimum amount of PII necessary to help perform functions that they are authorized to perform as assisters.
    b. Will ensure that the consumer's PII is kept private and secure and will follow privacy and security standards.
    c. May follow up about applying for or enrolling in coverage after first meeting with the consumer if consumers choose to provide their contact information.
    d. Might share the consumer's PII if referring the consumer to another source of help, with the consumer's permission.
    e. Will provide the consumer with copies of the completed authorization form and the Navigator's, EAPs or CAC's roles and responsibilities.
5. Exceptions or limitations to consents, including an acknowledgment that the consumer may revoke any part of the authorization at any time, as well as a description of any limitations that the consumer wants to place on your access to or use of the consumer's PII.
6. Include an expiration date or event, unless effectively revoked in writing by the consumer before that date or event.
7. Signature and space for consumer to provide contact information for follow-up, if desired.

Though not strictly required, we also strongly recommend including the following in the consent and/or in your standard procedures or forms for obtaining consumer consent:

1. An explanation of what PII includes and examples of the kinds of PII you might request from the consumer.
2. An acknowledgment that the consumer isn't required to provide you with any PII.
3. An explanation that the help you'll provide is only based on the information the consumer provides, and if the information given is inaccurate or incomplete, you might not be able to help the consumer in all situations.
4. An acknowledgment that you'll ask only for the minimum amount of PII necessary for you to carry out your functions and responsibilities.

Authorization Form Best Practices

Authorization forms should be written in plain language, and you should explain them verbally to consumers before they sign (or verbally consent, but you must record in writing that the consumer's authorization was obtained). When it is necessary to ensure meaningful access to health benefits for persons with limited English proficiency (LEP), authorization forms and materials must be translated and made available in the languages spoken within the community being served (including but not limited to consumers with LEP and/or those who communicate through American Sign Language (ASL)). Translated authorization forms and materials should be provided in simple, understandable language at an appropriate literacy level, preferably at the fourth-grade level. If translated authorization forms and materials aren't available, this material should be explained in the primary or preferred language of the person being assisted, which may require use of a qualified interpreter or qualified bi-lingual/multi-lingual staff person. You should explain that if consumers agree, you're permitted to access their PII to carry out your required or authorized assister duties, like helping them enroll in coverage through the FFMs.

Record of Authorization

You must keep a record of the consumer's authorization, which could include the consent form used by your organization. At a minimum, the record of the authorization must include:

1. The consumer's name and (if applicable) the name of the consumer's legal or Marketplace authorized representative.
2. The date the consent was given.
3. Your name or the name of the assister to whom consent was given.
4. Notes regarding any limitations placed by the consumer on the scope of the consent.
5. Notes recording all acknowledgments and consents obtained from the consumer.
6. If any changes are later made to the authorization, including if and when a consumer revoked the consent or any part thereof.

Retention Period

In FFMs, the minimum amount of time your organization needs to keep a record of consumers' authorization is six years unless a different and longer retention period has been provided under other applicable federal or state law.

Expiration of Consent

Consumers' consent may last indefinitely unless they revoke it, or your organization chooses to set its own expiration date for consumer consent. Under CMS regulations, you must permit consumers to revoke their consent at any time, which includes permitting consumers to place a time restriction on the consent at any time.

Ways to Obtain Consumer Consent

Consumers may give consent themselves or choose to have a legal or authorized representative provide consent on their behalf. However, a legal or authorized representative must have authority to act on a consumer's behalf.

You may obtain a consumer's general consent (e.g., over the phone, in writing, or both) to access their PII to carry out authorized assister functions as long as a record of the consent is maintained consistent with FFM requirements. To use PII for purposes unrelated to your authorized assister functions, you must obtain the consumer's informed consent in writing. The consent must include the specific elements set forth in the privacy and security standards that apply to you and your organization.

Consent for Multiple Assisters

It isn't necessary for a consumer to provide a separate consent for each individual assister in an assister organization. Generally, a consumer's consent includes permission for any assister affiliated with your organization to access the consumer's PII for authorized assister functions. The CMS model consent forms clarify that the consumer's consent extends to multiple assisters from the same organization in the General Consent section.

CMS.gov Model Authorization Form for FFM Navigators webpage.

CMS.gov Model Authorization Form for CACs webpage.

Knowledge Check

What elements does CMS require you to get when obtaining a consumer's consent?

Answer: The consent must cover at least the following elements: an acknowledgment that you'll inform the consumer of the functions and responsibilities that apply to your specific assister role, including all the consumer protection standards that apply through CMS regulations to your assister type (e.g., conflict-of-interest requirements, rules about accepting payment and providing gifts); consent for you to access and use the consumer's PII to carry out your Marketplace functions and responsibilities; the expiration date of consent; an acknowledgment that the consumer may revoke any part of the consent at any time; and a description of any limitations the consumer wants to place on your access or use of their PII.

Restrictions on Your Use of Consumers’ PII

Now that you've learned about obtaining consumers' consent, let's discuss some important restrictions on how you can use consumers' PII:

- You can't request or require an SSN or information regarding citizenship, status as a national, or immigration status for any consumers who aren't seeking coverage for themselves on any application, unless the consumer has separately provided informed consent in writing for you to access this information.
- You can't request information from or concerning any individual who isn’t seeking coverage for themselves, unless the information is needed for the Marketplace to determine an applicant's eligibility for enrollment in a QHP or an insurance affordability program or is required as part of a Small Business Health Options Program (SHOP) employer application.
- You can't collect PII beyond what is necessary to perform your authorized functions without the specific, informed consent of the consumer.
- You can't use PII to discriminate against consumers, like refusing to assist individuals who are older or who have complex health care needs.

Privacy Practices Recap

To protect consumers' privacy, your organization should:

- Establish and follow policies and procedures in compliance with privacy, security, and confidentiality standards.
- Follow all applicable restrictions related to the use and disclosure of personal information.
- Implement reasonable safeguards to ensure confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

As an assister, you must:

- Protect consumers' personal information from unauthorized use or disclosure.
- Make sure that anyone who has access to consumers' PII, which has been provided by the assister, keeps this information private and secure.

The FFMs place a high value on privacy to maintain consumers' trust. You can reassure consumers that their sensitive and personal information is safe with the FFMs. Consumers can access the FFM Privacy Policy to learn:

- How their PII and other personal information is used or shared by the FFMs.
- Protections in place to prevent consumers from having their personal information used or shared in a harmful way or in a manner not authorized by federal law.

Other State and Federal Laws that may Apply

Remember, you must comply with all other applicable state and federal laws related to the privacy and confidentiality of PII. It's your responsibility to understand which privacy and security laws and regulations apply to your role in the FFMs and to fully comply with those laws.

States may establish their own laws or regulations governing the activities of Marketplace assisters as long as those laws don't prevent the application of Title I of the Affordable Care Act (ACA). Several states have passed laws and implemented regulations that impose additional requirements on assisters.

Other State and Federal Laws that may Apply (Cont'd.)

You and your organization may create, collect, disclose, access, maintain, store, and use consumer PII to perform functions related to carrying out additional duties that may be required under applicable state law or regulations as long as the state requirement doesn't prevent the application of Title I of the ACA. Also, your organization must notify consumers in advance in writing that you might be required to use their PII to comply with a state law or regulation.

Given ongoing legislative, regulatory, and judicial actions related to state requirements, it's important to be aware of any additional requirements in the state(s) where you'll operate. For more information about your state-specific requirements, refer to your state Department of Insurance (DOI) or other state agency that regulates your activities as an assister.

Knowledge Check

Protecting the privacy and security of consumer PII is a crucial component of your role as an assister. What are the requirements under CMS regulations and assister privacy and security standards to protect consumer privacy and PII?

Answer: CMS regulations require you to obtain general consumer consent to access the consumer's PII to carry out authorized assister functions. You may do this verbally or in writing, and you must keep a record of the consumer's consent. The standards also require your organization to monitor for and report privacy and security breaches and to provide a Privacy Notice Statement, including prominently displaying it on any public-facing websites used to gather or request consumer information. You're permitted to collect a consumer's name, mailing address, email address, or telephone number without first providing a written Privacy Notice Statement if the contact information is only used to follow up with the consumer to perform an authorized function, like scheduling an appointment for application assistance, or to send the consumer educational information that is directly relevant to authorized assister functions.

How to Protect PII

Social Media

You can mention your role as an assister on Facebook, Twitter/X, and YouTube, but we recommend that you keep your references generic, like letting people know the location where you'll be available for assistance. Don't mention any private information, like consumers' specific names or medical conditions, without a consumer's specific, written consent to do so.

Direct Outreach

- Direct-contact outreach and education activities may include:
- Providing brochures and informational materials about the FFMs.
- Providing information on the annual FFM redetermination process.
- Informing consumers of application and enrollment assistance provided by your organization.

Remember, it is against federal law to place outreach or educational materials directly into a consumer's mailbox.

Contact Cards

If a consumer gives you contact information, like by filling out a contact card, this is considered consumer consent for future contact as long as the consumer was made aware the information might be used for future contact. However, you should obtain complete authorization if and when you follow up with the consumer in accordance with your organization’s standard authorization procedures.

Demographics

Unless the consumer you’re assisting specifically consents in writing, don't maintain additional client or demographic information beyond what is necessary to successfully perform authorized assister functions.

Appointments

You can keep certain client information, like name, email address, or phone number, if the consumer consents and it's necessary for making or maintaining an appointment or carrying out authorized assister functions.

Sign-up Sheets

Your organization might want to use sign-up sheets at your service location or when participating in an outreach or enrollment event so consumers who desire follow-up contact from the assister organization can leave their names and contact information.

Remember, you're permitted to collect a consumer's name, mailing address, email address, or telephone number without first providing a written Privacy Notice Statement if the contact information is only used to:

- Follow up with the consumer to perform an authorized function, like scheduling an appointment for application assistance; or
- Send educational information to the consumer that is directly relevant to authorized assister functions.

Door-to-Door Outreach: What’s New

Beginning June 18, 2023, under federal regulations, you’re now no longer prohibited from going door to door or use other means of direct contact, like a phone call, for the purpose of providing application or enrollment assistance to consumers, even if they haven't requested or initiated the contact or if you or your organization don’t already have a relationship with the consumer. For example, you can offer to help a consumer with an application or enrollment while conducting outreach by going door-to-door or offer to schedule an appointment for application or enrollment assistance while conducting outreach by going door-to-door.

However, you must make sure that you're complying with any other federal, state, or local laws that may apply to these interactions. Also, for safety purposes, CMS recommends you conduct door-to-door activities in groups of two or more.

Best Practices to Protect PII

Remember that a consumer's general consent typically permits you to create, collect, disclose, access, maintain, store, and use the consumer's PII only to the extent necessary to perform your authorized assister functions.

If, for example, a consumer provides their preferred contact information on a sign-up sheet, you'll have limited consent to use said contact information only to follow up or set up an appointment with that consumer. You may not retain any other PII for later use.

In-Person (Office)

- Make sure consumers take possession of their documents. However, you can provide postage materials and/or mail a paper application on a consumer's behalf as long as the consumer consents to the assister's retaining the application for this purpose. You can add a specific consent to the Navigator or CAC model authorization form so that consumers can consent to having their application mailed on their behalf.
- Secure hard-copy consumer consent forms in a locked location. Don't leave forms unattended in a room or car.
- Restrict access so only authorized individuals have access to PII and/or are allowed in areas where PII may be accessed.
- Maintain employee awareness and train employees on how to safeguard PII.
- Make sure that all scanning and copying equipment that may be used by consumers doesn't electronically retain copies of the images.
- Dispose of PII in a manner consistent with FFM rules and retention requirements.
- If consumers leave documents containing PII with you by accident, you should store the documents in a safe, locked location and return the documents to them as soon as possible.
- During consumer appointments, utilize private spaces to ensure privacy. If you're at an event and a private space isn't available, create a space that is out of earshot to discuss private information with potential applicants. Also, use computer screen covers to help protect PII from the view of others.
- PII collected from a consumer—including name, email address, telephone number, application ID number, addresses, or other notes—must be stored securely.
- If you work with other organizations, in your work with the FFM, you'll remain legally bound by and responsible for all obligations to protect consumers' PII. You're required to obligate the other organization to the same privacy and security standards that you must legally follow.

For more information, review the

CMS.gov resource Obtaining Consumer Authorization and Handling Consumers' PII in the FFM.

Electronic

- Verify that “auto-fill” settings on your Internet browsers are turned off.
- Maintain computer security, including the use of a secure wireless network, when performing assistance using an authorized mobile device (e.g., a tablet).
- Don’t send or forward emails with PII to personal email accounts (e.g., Yahoo or Gmail).
- Protect emails that contain PII (e.g., use encryption).
- Don’t upload PII to unauthorized websites (e.g., wikis).
- Don’t use unauthorized mobile devices to access PII.
- Lock up portable devices (e.g., laptops or cell phones).
- Clear your web browser history to avoid other users accessing PII.
- If in electronic format, PII should be stored securely in a password-protected file on a password-protected computer to which only authorized individuals have access.

For more information, review the

CMS.gov resource Obtaining Consumer Authorization and Handling Consumers' PII in the FFM.

Privacy, Security, and Confidentiality

After you obtain consumers' PII, you must utilize certain safeguards to secure PII regardless of whether it's held or transferred in hard copy or electronic form. Privacy and security go hand in hand to protect consumers' PII and confidential information. Select each term to learn more.

Privacy

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

Security

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

Confidentiality

Confidentiality means respecting your limitations when accessing or disclosing a consumer's information. You should abide by relevant laws and safeguard consumers' personal privacy and proprietary information.

Privacy Practices

The Department of Health and Human Services (HHS) oversees and monitors entities that are required to comply with Marketplace privacy and security standards, including FFM assisters. HHS may conduct audits, investigations, inspections, and other activities related to its oversight of compliance with FFM privacy and security standards.

Unauthorized or inappropriate uses or disclosures of PII can result in civil, criminal, or administrative proceedings or actions. All Marketplaces, including the FFMs, are required to have privacy and security standards.

The FFMs establish assister privacy and security standards through agreements with “non-Exchange entities,” like Navigator grantees, EAPs, and CAC designated organizations (CDOs).

Individual CACs in an FFM should refer to their agreements with their CDOs since these agreements must include the privacy and security standards established by the FFMs.

Examples of these agreements include:

- Standard Grant/Cooperative Agreement Terms and Conditions for Navigator Grantees in the FFMs.
- CMS-CDO Agreements.

Navigator, EAP, and CAC Security Requirements

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

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

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

Knowledge Check

What are examples of practices you'll follow with respect to PII in the FFMs?

Answer: You must inform consumers of your or your organization's collection and use of their PII by obtaining their consent both for general purposes related to your authorized functions and for any specific uses that go beyond those authorized functions, regardless of whether or not consumers request an explanation. You must also provide them with a Privacy Notice Statement. You must allow consumers to revoke any part of their consent at any time or allow them to place limits on your access to or use of their PII. Take appropriate steps to safeguard the confidentiality of PII. Privacy breaches should be reported to the CMS Information Technology (IT) Service Desk.

Knowledge Check

What is not allowed for direct-contact outreach and education activities for assisters and navigators?

Answer: It is against federal law to place outreach or educational materials directly into a consumer's mailbox. Assisters and Navigators are no longer prohibited from going door-to-door to provide enrollment assistance even if the consumer has not requested or initiated contact or if you or your organization don't already have a relationship with the consumer. You are also allowed to maintain information regarding a client and/or their demographic for what is necessary to perform authorized assister functions.

Knowledge Check

Hi, I’m Sunny, an independent house cleaner. I am very concerned about the privacy of my personal information. What steps will you take to protect my privacy?

Answer: You should tell Sunny how you work to protect her privacy, including telling her and giving her a list in writing of what information might be collected, why it's collected, and how it will be used and shared for you to help her as an assister. In the FFMs, the minimum amount of time your organization needs to keep a record of consumers’ consent is six years, unless a different and longer retention period has been provided under other applicable federal law. If you retain any consumer PII, you must always get the consumer's consent first, before providing them with any assistance.

Key Points

- PII is a type of information that can be used to distinguish or trace a consumer's identity alone or when combined with other personal or identifying information that is linkable to a specific individual.
- If you retain any consumer PII, you must always get the consumer's consent first and maintain PII privately and securely in a manner that complies with privacy and security standards that apply to you and your organization.
- You may use or disclose PII as needed to carry out required or authorized assister functions.
- You’re no longer prohibited from going door-to-door or use other means of direct contact, like a phone call, for the purpose of providing application or enrollment assistance to consumers, even if they haven't requested or initiated the contact or if you or your organization don’t already have a relationship with the consumer.

Module 3 - Handling Privacy and Security Incidents and Breaches

Introduction

What happens when security safeguards aren’t in place? By the end of this module, you’ll understand the following concepts and be able to accomplish the tasks below them.

Key Terms

Define the terms security incident, privacy incident, and breach.

Compromised Personally Identifiable Information (PII)

State the steps to take if a consumer's PII is compromised.

Consequences

State the consequences of failing to protect a consumer's PII.

Privacy and Security Incidents

Security incidents are a potential threat to the confidentiality, integrity, or availability of PII. A security incident is the act (or attempt) of violating an explicit or implied security policy, which includes attempted or successful unauthorized access, use, disclosure, modification, or destruction of data or interference with system operations in an information system.

A privacy incident is a security incident where unauthorized individuals gain access to PII.

Privacy incident scenarios include:

- Losing encrypted or unencrypted electronic devices that contain PII (for example, laptops, cell phones, disks, thumb drives, flash drives, and CDs).
- Losing hard-copy documents containing PII.
- Sharing paper or electronic documents containing PII with individuals who aren't authorized to access it.
- Accessing paper or electronic documents containing PII without authorization or for reasons not related to job performance.
- Emailing or faxing documents containing PII to inappropriate recipients, whether intentional or unintentional.
- Posting PII to a public-facing website, whether intentional or unintentional.
- Mailing hard-copy documents containing PII to the incorrect address, whether intentional or unintentional.
- Leaving documents containing PII exposed in an area where individuals without approved access could read, copy, or move it for future use.

Knowledge Check

What would be considered a privacy incident?

Answer: Misplacing a mobile device that contains PII, losing PII data through theft, and misrouting an email message containing PII would all be privacy incidents since they all involve the improper and unauthorized disclosure of PII. Overhearing a conversation in the hallway isn't a privacy incident.

What Is a Breach?

A breach is a privacy incident that poses a risk of harm to applicable individuals. The determination of whether a Centers for Medicare & Medicaid Services (CMS) privacy incident rises to the level of a breach is made exclusively by the CMS Breach Analysis Team (BAT).

If you learn of a situation in which a consumer's PII has been compromised in any way, including unauthorized persons viewing or possessing the information or losing the records, the incident should be reported to CMS within one hour of discovery.

Because your organization is approved to aid consumers, it should have written procedures in place for addressing privacy and security incidents.

File a Breach Report

What types of issues should be reported?

- Lost, stolen, or misplaced records or computers
- Unauthorized personnel or other third parties viewing or possessing PII information
- Incidents having the potential to compromise consumer information

Assister organizations must implement and comply with breach and incident handling procedures consistent with CMS's Risk Management Handbook that details the identification, response, recovery, and follow-up of incidents and breaches.

These procedures must be in writing, address how to identify incidents, and identify the assister organization's designated personnel (for example, a privacy official or officer) responsible for reporting and managing incidents or breaches to CMS.

These procedures require the reporting of any incident or breach of PII to the CMS Information Technology (IT) Help Desk within one hour after discovery of the breach or incident:

- By telephone: 1-410-786-2580 or 1-800-562-1963.
- Via email (within required timeframes): cms_it_service_desk@cms.hhs.gov.

Knowledge Check

What types of incidents must be reported in a manner consistent with the CMS incident and breach notification procedures?

Answer: If you accidentally leave a file folder containing PII in a public location or your office manager shares information about one consumer with another person without the consumer's consent, you could be putting your consumers at risk of identity theft or otherwise having their privacy violated.

Consequences of Not Protecting PII

What do these things have in common?

Stolen Identity

Loss of Trust

$25,000 Fine

Termination

Civil Money Penalty

They are all examples of the consequences of failing to protect consumers' PII.

It's important to protect PII so consumers feel that they can trust you with their personal information, to make sure consumers aren't exposed to personal risk, and to protect yourself. If you don't protect PII or disclose it inappropriately, you may cause harm to consumers, face disciplinary action by your organization, and be at risk for a civil money penalty (CMP) * by the Federal Government. If you fail to protect consumers' information and/or purposefully disclose their PII for an unauthorized purpose, any of the following might occur:

- Consumers' identities may be stolen.
- You may lose consumers' trust because they are sensitive about sharing their personal information.
- You won't be following the standards of the Federally-facilitated Marketplaces (FFMs).
- You may have to pay a CMP, commonly called a “fine”, of up to $25,000 per violation under the Affordable Care Act (ACA).
- You or your organization may be terminated from providing CMS-authorized assistance to consumers enrolling in health coverage through the FFMs.

***Note: Civil Money Penalty**

The Department of Health & Human Services (HHS) can impose a CMP if you knowingly and willfully use or disclose consumers' PII in any way that violates federal law and the FFM's privacy and security standards. When determining the amount of the CMP, HHS may consider factors like the nature and circumstances of the violation and the actual or potential harm caused by the violation.

Knowledge Check

You have been helping Julio and Sue enroll in coverage through the FFM. While finishing their application in your office today, they ran out quickly when they got a phone call from their babysitter. In their rush, they unintentionally left their paper tax returns containing information, including their Social Security Numbers (SSNs), names, addresses, and phone numbers on your desk. What should you do?

Answer: You should follow the couple with the papers, hoping you can catch them and return the papers. If you're unable to find them, you should attempt to contact them to ask that they retrieve their papers. In the meantime, you should store the documents in a safe, locked location and return the documents to them as soon as possible.

Key Points

- A privacy incident occurs anytime people have access or potential access to PII when they're not authorized to or when they use PII for an unauthorized purpose. A privacy incident can arise from a number of causes.
- A breach is a privacy incident that poses a reasonable risk of harm to the applicable individuals. Any suspected breach should be reported immediately.
- You must report all PII incidents and breaches to the CMS Information Technology Service Desk within one hour after discovery of the breach or incident.

Module 4 - Reducing Threats and Risks

Introduction

Now that you understand your responsibility to report privacy incidents and breaches, let's discuss reducing risk using information security. By the end of this module, you should understand the following concepts and be able to accomplish the tasks below them.

Key Terms

Define information security.

Computer Threats

List potential threats to a computer.

Organizational Controls

List controls an organization should use to protect information technology assets.

Password Protection

List password protection techniques.

Information Security Overview

What is information security?

Information security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

- Information security is achieved through implementing technical, management, and operational measures designed to protect the confidentiality, integrity, and availability of information.
- The goal of an information security program is to understand, manage, and reduce the risk to information under the control of the organization.
- In today's work environment, many information systems are electronic; however, the Department of Health & Human Services (HHS) has a media-neutral policy toward information. This means that any data must be protected, whether it is in electronic, paper, or oral format.

Knowledge Check

What best describes information security?

Answer: Information security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Threats to Your Computer

It's essential that any computers you use are protected from harmful computer programs, applications, and malware (malicious software). It's your responsibility to make sure that computers in your office used by consumers to access the FFMs are regularly updated with the latest security software to protect against any cyber-related security threats.

You may occasionally assist consumers using public computers (like those in libraries). In these instances, you should never save private files to a public computer to upload to an application because it could lead to PII being mistakenly disclosed.

Malware is software designed to harm or secretly access a computer system without the owner's consent. It's a generic term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Email and corrupted websites may deliver malware that infect computers used to access the FFMs. Public computers, like those accessed in a library, may be susceptible to malware and viruses.

Controls

You can apply certain controls to protect information within the FFMs. Controls are policies, procedures, and practices designed to manage risk and protect Centers for Medicare & Medicaid Services (CMS) Information Technology (IT) assets.

Common examples of controls include:

- Security awareness and training programs.
- Physical security like guards, badges, and fences.
- Restricting access to systems that contain sensitive information.

Your organization is required to monitor, periodically assess, and update its security controls and related system risks to maintain continued effectiveness of those controls.

Password Protection Tips

Some examples of steps you can take to help promote information security on information systems that may store consumer PII include:

- Changing your password often;
- Changing your password immediately if you suspect it has been compromised;
- Using a different password for each system or application;
- Choosing a password that isn't generic and easily obtained like family member names, pet names, birth dates, phone numbers, or vehicle information; and
- Never sharing your password with anyone.

Knowledge Check

What is an information security best practice?

Answer: When choosing your password, don’t use generic information that can easily be obtained, like family member names, pet names, birth dates, phone numbers, or vehicle information.

Key Points

- Information security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
- You must make sure that any computers you use to store consumer PII are protected from harmful computer programs, applications, and malware and are regularly updated with the latest security software to protect against any cyber-related security threats.
- Other examples of steps you can take to promote information security in the FFMs include changing passwords often, using different passwords for each system or application, and not sharing your password with others.

Module 5 - Fraud Referrals

Introduction

People seeking to commit fraud may intentionally submit or provide false or misleading information to the Federally-facilitated Marketplaces (FFMs) and/or consumers. In addition, they may falsely claim to be certified to offer consumer assistance with the FFMs to gain access to consumers' personal information.

While this isn't expected to happen often in the FFMs, it's important for you to be familiar with how to identify potential fraud and what to do when you think fraud may have occurred. Committing fraud is a serious offense. By the end of this module, you should be able to understand the following concepts and accomplish the tasks below them.

Key Terms

Define fraud.

Examples in the Marketplaces

Describe examples of fraud in the Marketplaces.

Protecting Personally Identifiable Information (PII)

List techniques consumers should use to protect their PII.

Role of Assister

Describe the assister’s role in preventing fraud.

Reporting Fraud

Describe the process for reporting fraud.

Definition of Fraud

In your work, you may become aware of fraud committed by:

- A consumer.
- A health insurance company.
- An agent, broker, or assister.
- Another individual or organization.

While many of these individuals and entities are committed to providing accurate information and unbiased FFM enrollment assistance, some may have the intention to commit fraud against consumers, the government, or both.

Fraud, as the term is used in this training, happens when an individual or an entity (for example, a business) deliberately omits or mis-states important information for personal benefit.

Examples of Fraud in the Marketplace

You should recognize behaviors or situations that may be examples of fraud and report them to the proper authorities. It's not your responsibility to prove that fraud occurred. Fraud may be committed in different ways in connection with the FFMs. Select each situation below to identify the different ways people may commit fraud.

Fraud Committed by a Consumer

Consumers could give false information to qualify for certain types of benefits provided by the FFMs or other government entities. Consumers may knowingly misrepresent facts (for example, personal financial information or number of dependents) to get coverage through Medicaid or Children's Health Insurance Program (CHIP) or to get a more favorable premium tax credit or more favorable cost-sharing reductions (CSRs) through the FFMs.

Other examples include consumers who knowingly:

- Fail to report all sources of income on their eligibility applications.
- Don't disclose that they use tobacco on their eligibility applications.
- Provide false identifying information like a false name or SSN or intentionally misrepresent their household income.

Fraud or Misrepresentation Committed by a Health Insurance Company

A health insurance company could give false information in an attempt to convince consumers to enroll in its health plan or to not enroll consumers if insuring them could be expensive. A health insurance company might also promise consumers certain services or prices, but then not offer them the services or prices once they enroll.

Fraud Committed by an Agent or Broker

Examples of fraud that could be committed by an agent or broker include:

- Misrepresenting information to convince consumers to enroll in a health plan the agent or broker represents.
- Knowingly promising consumers certain services or prices that aren't actually available.
- Representing that they work for the FFMs in order to obtain consumers' personal information.
- Using false information to steer a consumer to a particular health insurance company's health plan.
- Enrolling a consumer in a health plan without the consumer's knowledge or consent.
- Enrolling a consumer in duplicative coverage to obtain another commission or other financial benefit.

Fraud Committed by Another Individual or Organization

Another organization or individual may falsely represent that they're certified to help people enroll through the FFMs by claiming to be an agent, broker, or assister. That individual could email or otherwise contact consumers, asking for their personal information in order to enroll them in a qualified health plan (QHP) through the FFMs.

Knowledge Check

What are examples of potential fraud?

Answer: Examples of fraud include the following: when consumers intentionally misrepresent their tobacco use; when a business claims to offer QHPs without being authorized by the FFMs to do so; and when consumers intentionally report dependents when they actually have none. Accidentally providing inaccurate information is important to correct but isn't considered fraud.

What You Should Tell Consumers

To protect themselves against fraud, you should encourage consumers to follow a few basic guidelines related to the FFMs.

Consumers Should:

- Protect their SSN by only providing it to trusted assisters or websites.
- Shred documents containing health care information or other personal information before throwing them away.
- Look for official .gov Web addresses which will have logos for HHS and HealthCare.gov.
- Be an informed consumer and take the time to compare coverage options before deciding.
- Review information from health plans to make sure only services, equipment, and prescriptions used by consumers or their household members are listed on an Explanation of Benefits (EOB).
- Be wary of product promotions, so-called "special deals," or other offers that seem too good to be true because these offers may be related to fraud or identity theft.
- End any suspicious call or visit immediately.
- Report suspicious calls or visits to your state Department of Insurance or the FFM Call Center.

Consumers Should Not:

- Give out personal information over the telephone, the Internet, or in person unless the requestor has proven they have the authority to gather this information (for example, an insurance company or the FFM) for enrollment purposes.
- Sign blank insurance forms or applications.
- Be pressured into making purchases, signing contracts, or committing funds.
- Be afraid to ask questions and verify the answers.

Your Role Against Fraud

You can also play a role in fighting fraud by:

- Protecting consumers' private health care and financial information and reminding them to be cautious when giving out their Social Security Numbers (SSNs), credit card numbers, or banking information.
- Encouraging consumers to accurately answer application questions.

Consumers' SSNs, if available, should be provided only to the FFMs and will be used for the following purposes:

- To determine if consumers are eligible for health coverage.
- To share with the health insurance company offering the plan selected by the consumers.
- To assist consumers with getting help paying for coverage.
- To verify immigration status.

Remember, you and the FFMs can only request SSNs from consumers who aren't seeking coverage when that information is necessary for another individual's eligibility determination for enrollment in a QHP, insurance affordability program, or as part of a Small Business Health Options Program (SHOP) employer application under 45 CFR 155.731. Individuals aren’t required to provide SSNs; however, they can help speed up the verification process by providing SSNs for all consumers whose incomes are included from their household on an individual market FFM application.

You should also reassure consumers it's your job to provide accurate and impartial information and that you can help them access the resources they need to make informed decisions about getting coverage through the FFMs.

Information Needed to Report Suspected Fraud

If consumers feel they have experienced fraud or have been the victims of identity theft, you're encouraged to help them report this to the appropriate authorities. In all situations of suspected fraud, it's important to collect as much information as possible so you or the consumer can accurately report it.

Types of information to collect may include:

- The name or ID number of the individual or entity suspected of fraud.
- Contact information for the individual or entity suspected of fraud.
- A summary of the suspected fraud.
- The date the suspected fraud occurred.
- Whether you suspected the fraud or learned about it from a third party.
- If the third party was a consumer, you should include contact information for the consumer as well.

Reporting Process: Consumers as Victims of Fraud

Once you've collected the necessary information, you can report suspected fraud. Consumers who tell you they may be victims of fraud should be directed to report the incident to the appropriate authority.

For example:

- Refer consumers with complaints against agents or brokers to their state Department of Insurance or other state agency that regulates these entities.
- Direct consumers who believe their SSN or PII has been stolen to contact the Federal Trade Commission (FTC) by calling 1-877-382-4357 (1-877-FTC-HELP) or visiting the FTC website.

You can also:

- Direct consumers to contact the Social Security Administration (SSA) if they need help getting a new SSN.
- Help consumers avoid unsolicited offers by encouraging them to register their home and cell phone numbers with the National Do Not Call Registry online or by phone at 1-888-382-1222.
- Inform consumers they should review their EOB from their insurance company to check if they were billed for services or equipment they didn't receive.

Role of the Office of the Inspector General

If you believe a consumer falsified information to enroll in coverage through the FFMs, you should report the suspected fraud to the Fraud Hotline of the HHS Office of the Inspector General (OIG). Similarly, if a consumer believes someone else is using their information to get coverage, you're encouraged to help the consumer report the suspected fraud to the OIG Fraud Hotline. You may volunteer to assist with completion of the report.

The OIG will research each fraud referral report to determine if fraud actually occurred. The next steps they take may include discipline or referring the fraud incident to another agency or division within HHS. An HHS representative may follow up with you or the consumer for more information. It's important to provide as many details as possible in your initial report.

HHS takes every fraud complaint seriously and researches each one to determine whether fraud occurred. The time needed for a fraud investigation can vary greatly. It's not uncommon for a fraud investigation to take years. Since fraud complaints are often complex, HHS isn't able to confirm or deny the status of ongoing investigations.

It's important to note that all claims of fraud are confidential. No adverse action can be taken against you or a consumer for reporting suspicious behavior.

Reporting Consumer Fraud

You can submit a report of suspected fraud to any of the following entities:

HHS Office of the Inspector General (OIG):

Contact to report that a consumer's information was used to enroll someone else in the FFMs.

- Online: HHS OIG Fraud Hotline
- Phone: 1-800-HHS-TIPS (1-800-447-8477);
- TTY 1-800-377-4950
- Mail: HHS OIG

  ATTN: OIG HOTLINE OPERATIONS

  P.O. Box 23489

  Washington, DC 20026

Federal Trade Commission (FTC):

Contact to report identity theft.

- Online: Secure Complaint Form
- Phone: 1-877-ID-THEFT (1-877-438-4338); TTY 1-866-653-4261

State Department of Insurance (DOI):

Contact to report agent/broker fraud.

Contact your state DOI.

Marketplace Call Center:

Contact to report a complaint about an assister.

Contact to submit a complex case form.

- Phone: 1-800-318-2596; TTY: 1-855-889-4325 (all languages available)
- Assisters can report fraud by first calling the Marketplace Call Center and then submitting a complex case web form. A complex case is a case involving a single consumer or tax household where the assister has been unable to resolve a specific issue on the consumer or tax household’s application for Marketplace coverage. Complex cases are not policy questions or general questions about the Marketplace application. The complex case web form allows assisters to submit a complex case for investigation. In all cases except where a consumer was enrolled in a Marketplace plan or had their Marketplace plan switched without their consent, assisters must contact the Marketplace Call Center before submitting a complex case.

Knowledge Check

What is true about reporting a possible instance of fraud?

Answer: Fraud should always be reported immediately with as much information as possible. The HHS OIG will research each fraud referral form to determine if fraud occurred and take any next steps, including discipline or referring the fraud to another agency or division within HHS. All claims of fraud are confidential.

Key Points

- Fraud may be committed by consumers, health insurance companies, agents or brokers, or other individuals or organizations.
- You should take steps to recognize suspected fraudulent behavior and report it.
- You should encourage consumers to follow a few basic guidelines to recognize and prevent fraud in the FFMs.
- Any incidences of suspected fraud should be reported to the appropriate oversight organization by phone, email, fax, or mail.
- All fraud reports are confidential. Neither you nor your consumers will be penalized for submitting reports for investigation.

Conclusion

Awesome job! You learned about privacy and security standards applicable to the FFMs, including protecting consumer information and information security, consent requirements, handling privacy and security incidents and breaches, and identifying information security practices. You also now know how to recognize and prevent fraud.

You've finished the learning portion of this course. Select Exit Course to leave the course and take the Privacy, Security, and Fraud Prevention exam or to close the course and return to the exam later.

If you choose to take the exam, the code to access this exam is: 532049.

Resources

Note: There are some references and links to nongovernmental third-party websites in this section. CMS offers these links for informational purposes only, and inclusion of these websites shouldn't be construed as an endorsement of any third-party organization's programs or activities.

Module 2 – Protecting Consumer Information

Resources Page for Assisters on Marketplace.cms.gov: Technical assistance resources, including guidance and regulations on assister programs, tip sheets, and other resources for assisters, can be found on this assister resources page on Marketplace.cms.gov.

CMS.gov/marketplace/in-person-assisters/technical-resources/guidance-regulations

Consumer Authorization and Personally Identifiable Information (PII): Obtaining Consumer Authorization and Handling Consumers' PII in the FFM.

CMS.gov/marketplace/technical-assistance-resources/consumer-authorization-and-handling-pii.pdf

Health Insurance Marketplace Privacy Policy:

Healthcare.gov/privacy/

Module 3 – Handling Privacy and Security Incidents and Breaches

CMS Risk Management Handbook Chapter 08: Incident Response: This handbook addresses CMS' breach and incident handling procedures.

Security.cms.gov/policy-guidance/risk-management-handbook-chapter-8-incident-response-ir

Module 4 – Reducing Threats and Risks

Navigator Program Standards: Standards applicable to Navigators and Navigator grantees in Federally-facilitated Marketplaces.

ECFR.gov/current/title-45/subtitle-A/subchapter-B/part-155/subpart-C/section-155.210

Certified Application Counselor Standards: Standards applicable to certified application counselors and certified application counselor organizations in Federally-facilitated Marketplaces.

ECFR.gov/current/title-45/subtitle-A/subchapter-B/part-155/subpart-C/section-155.225

Module 5 – Fraud Referrals

National Do Not Call Registry Online: Official National Do Not Call Registry website where phone numbers can be registered, and complaints can be filed.

Donotcall.gov/

Office of the Inspector General (OIG) Fraud Hotline: OIG Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in the Department of Health and Human Services' programs.

OIG.hhs.gov/fraud/report-fraud/

Secure Complaint Form: Links to the Federal Trade Commission's online complaint assistant where consumers can report suspected fraud and abuse.

Reportfraud.ftc.gov/#/

Harmonized Security and Privacy Framework: Official CMS guidance on federal privacy and security requirements.

CMS.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Harmonized-Security-and-Privacy-Framework-ERA-Supp-v-1-0-08012012-a.pdf

Reporting Fraud:

CMS.gov/medicare/medicaid-coordination/center-program-integrity/reporting-fraud

Marketplace Call Center: Contact information for the Marketplace Call Center, 24 hours a day, 7 days a week for consumers needing assistance with fraud.

Healthcare.gov/contact-us/