Federally-facilitated Marketplace Assister Curriculum: Privacy, Security, and Fraud Prevention Standards

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

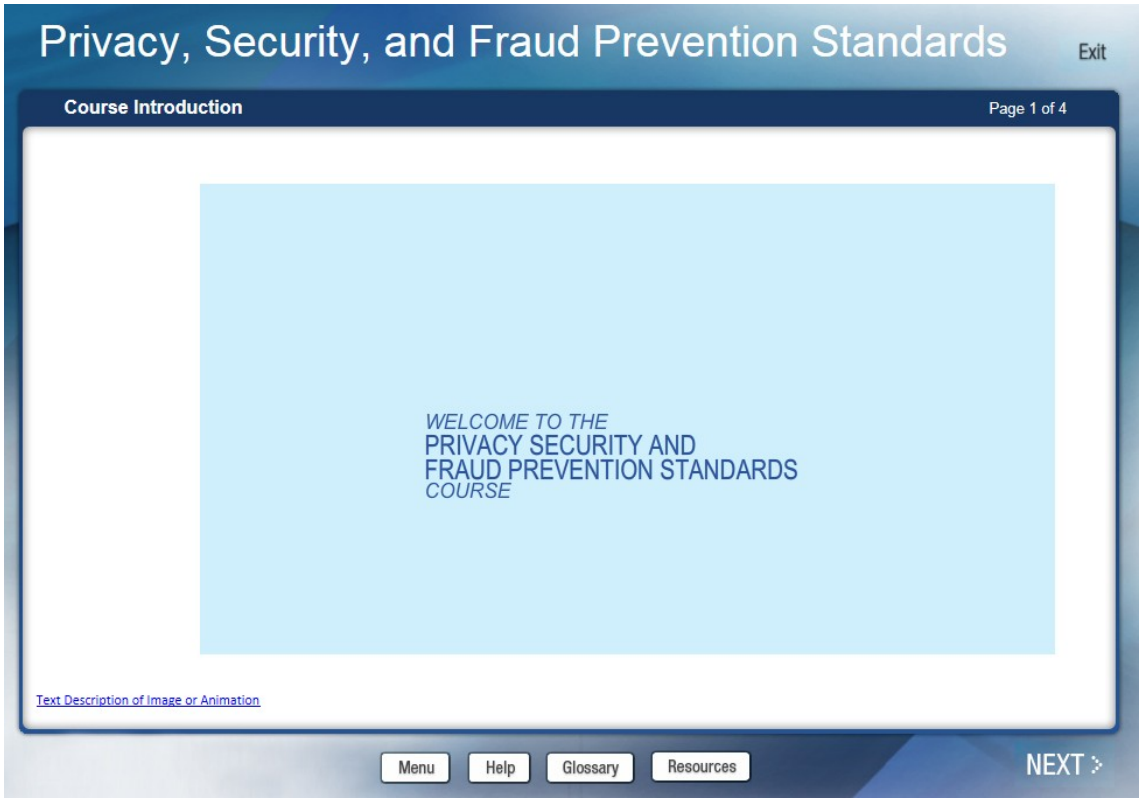
Center for Consumer Information & Insurance Oversight

November 2016

Table of Contents

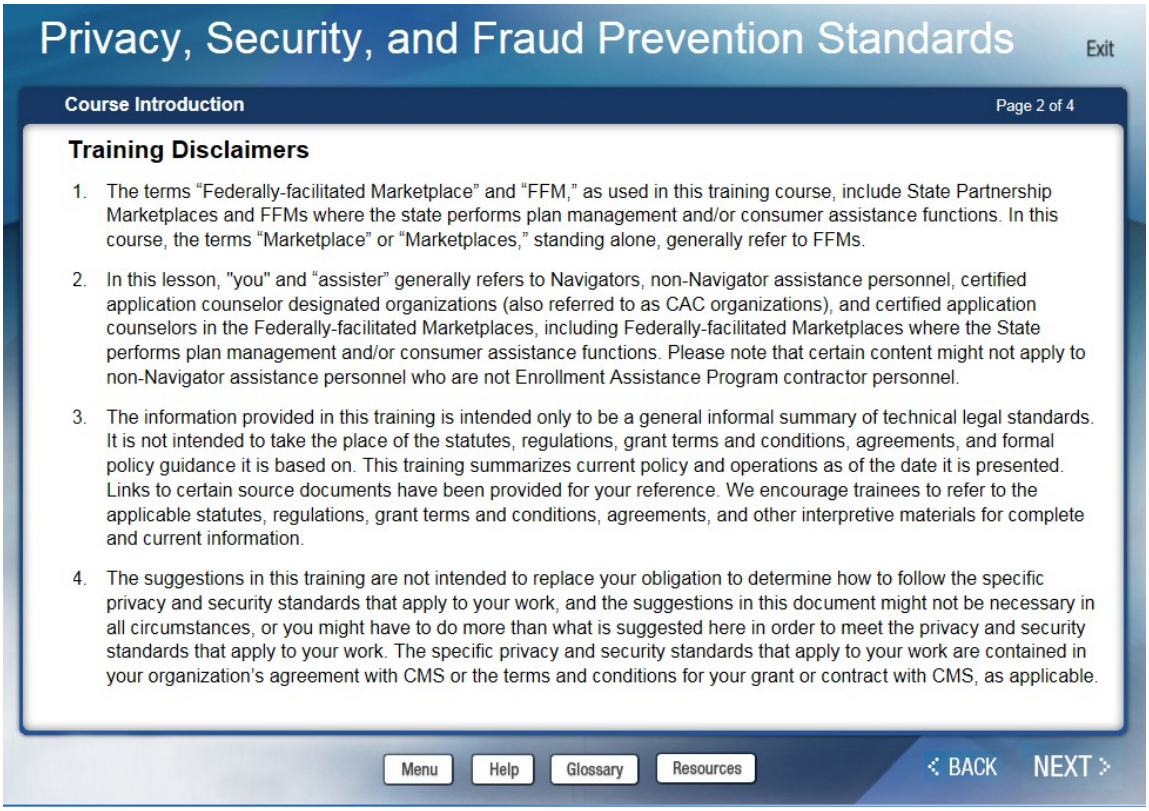
Privacy, Security, and Fraud Prevention Standards Course

Course Introduction Module



Course Title

Welcome to the Privacy, Security, and Fraud Prevention Standards Course

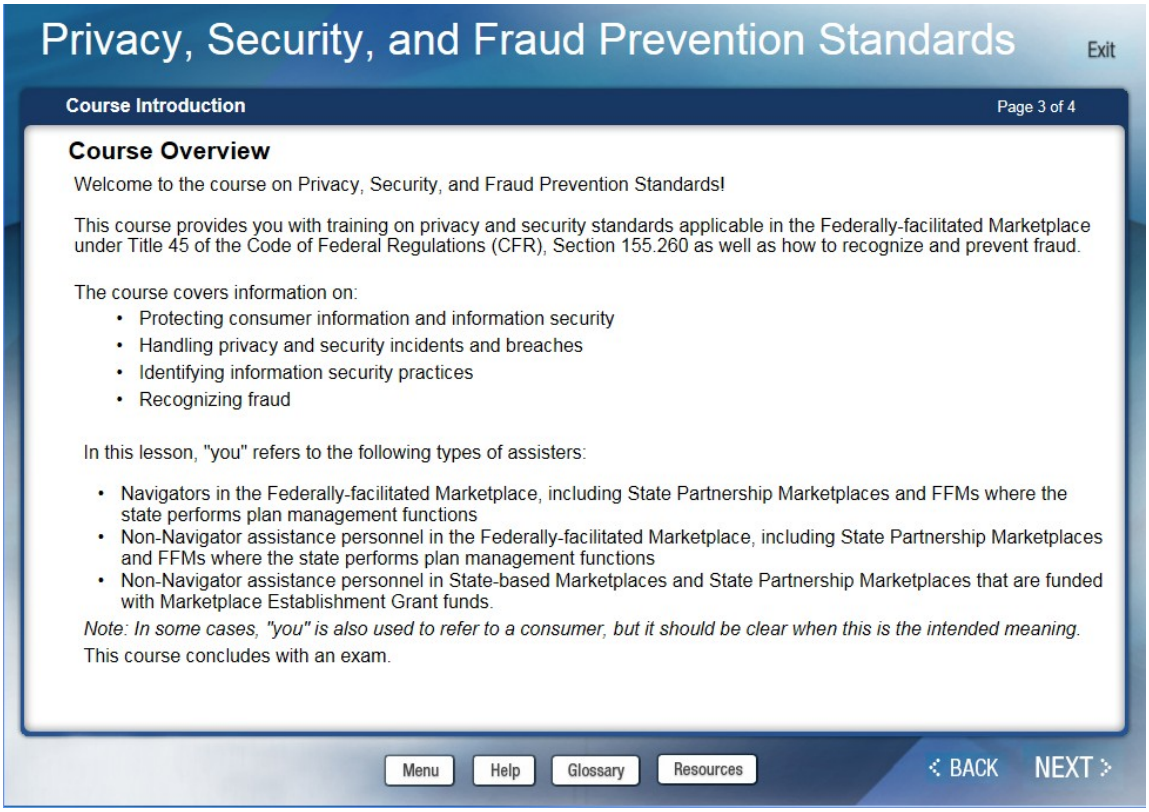


Training Disclaimers

1. The terms “Federally-facilitated Marketplace” and “FFM,” as used in this training course, include State Partnership Marketplaces and FFMs where the state performs plan management and/or consumer assistance functions. In this course, the terms “Marketplace” or “Marketplaces,” standing alone, generally refer to FFMs.
2. In this lesson, "you" and “assister” generally refers to Navigators, non-Navigator assistance personnel, certified application counselor designated organizations (also referred to as CAC organizations), and certified application counselors in the Federally-facilitated Marketplaces, including Federally-facilitated Marketplaces where the State performs plan management and/or consumer assistance functions. Please note that certain content might not apply to non-Navigator assistance personnel who are not Enrollment Assistance Program contractor personnel.
3. The information provided in this training is intended only to be a general informal summary of technical legal standards. It is not intended to take the place of the statutes, regulations, grant terms and conditions, agreements, and formal policy guidance it is based on. This training summarizes current policy and operations as of the date it is presented. Links to certain source documents have been provided for your reference. We encourage trainees to refer to the

applicable statutes, regulations, grant terms and conditions, agreements, and other interpretive materials for complete and current information.

4. The suggestions in this training are not intended to replace your obligation to determine how to follow the specific privacy and security standards that apply to your work, and the suggestions in this document might not be necessary in all circumstances, or you might have to do more than what is suggested here in order to meet the privacy and security standards that apply to your work. The specific privacy and security standards that apply to your work are contained in your organization's agreement with CMS or the terms and conditions for your grant or contract with CMS, as applicable.



Course Overview

Welcome to the course on Privacy, Security, and Fraud Prevention Standards!

This course provides you with training on privacy and security standards applicable in the Federally-facilitated Marketplace under Title 45 of the Code of Federal Regulations (CFR), Section 155.260 as well as how to recognize and prevent fraud.

The course covers information on:

- Protecting consumer information and information security
- Handling privacy and security incidents and breaches
- Identifying information security practices
- Recognizing fraud

In this lesson, "you" refers to the following types of assisters:

- Navigators in the Federally-facilitated Marketplace, including State Partnership Marketplaces and FFMs where the state performs plan management functions
- Non-Navigator assistance personnel in the Federally-facilitated Marketplace, including State Partnership Marketplaces and FFMs where the state performs plan management functions

- Non-Navigator assistance personnel in State-based Marketplaces and State Partnership Marketplaces that are funded with Marketplace Establishment Grant funds.

Note: In some cases, "you" is also used to refer to a consumer, but it should be clear when this is the intended meaning.

This course concludes with an exam.

Protecting Consumer Information Module

Introduction to Protecting Consumer Information

When you help consumers apply for health coverage through the Marketplace, you may have access to their personal information. It's important to make sure that you protect personally identifiable information (PII) when you're helping consumers.

This training will provide you with the skills to:

- Describe the difference between privacy, security, and confidentiality
- Recognize the ways to identify PII
- Explain how individuals may access and correct their PII
- Identify the extent to which PII may be created, collected, used, disclosed, accessed, maintained, and stored
- Describe key privacy responsibilities, restrictions, and best practices to protect PII in the Marketplaces

Privacy, Confidentiality, and Security

How are privacy, confidentiality, and security defined?

Privacy is consumers' rights to control how their personal information is used or disclosed.

Confidentiality means respecting any limitations on information access and disclosure according to relevant law and the consumers' wishes to protect their personal privacy and proprietary information.

Security refers to the safeguards (including systems and physical safeguards) in place to protect the privacy and confidentiality of personal information.

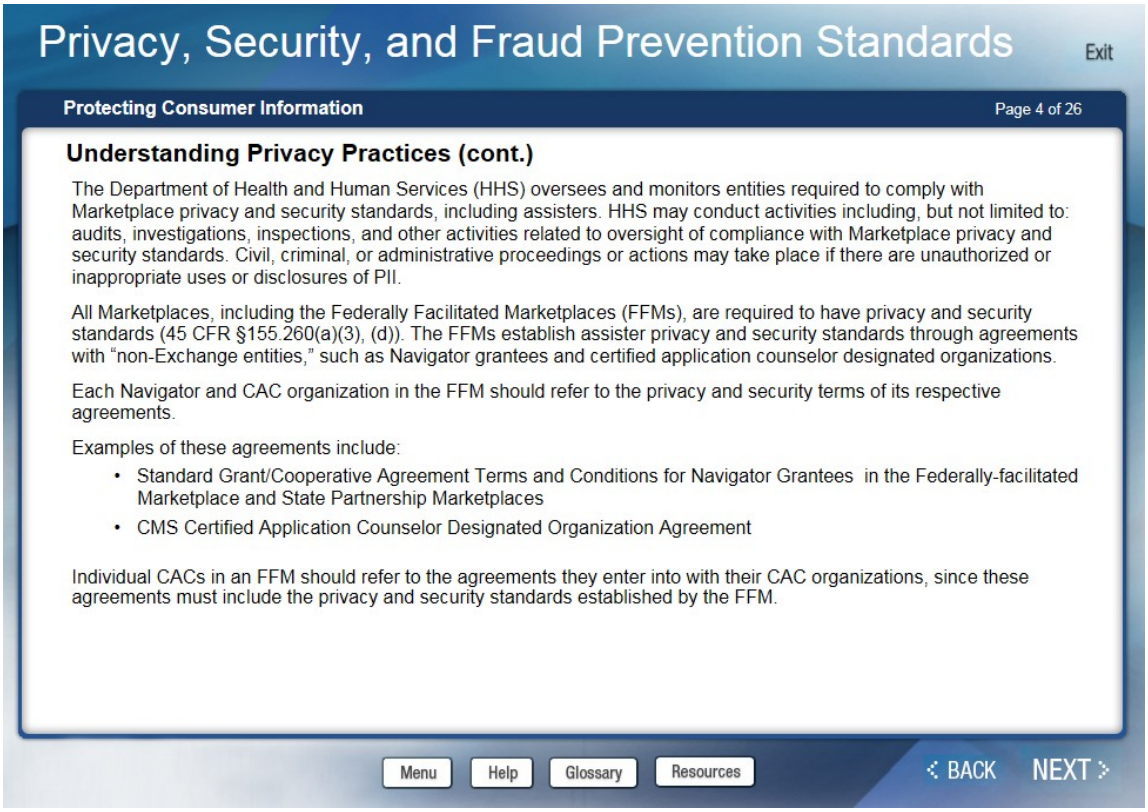
Privacy's success depends on establishing a basic foundation for information security. Establishing and following policies and procedures, as well as restrictions related to the use and disclosure of personal information helps to build a basic foundation for information security. Privacy and security go hand-in-hand to protect PII.

Understanding Privacy Practices

Information privacy involves protecting an individual's personal information from unauthorized use or disclosure. Protecting personal information is important to protecting an individual's privacy. By implementing privacy practices, you ensure that information is used only for its intended purpose. Anyone accessing PII has the obligation to ensure that the information remains private and secure.

The Marketplaces place a high value on privacy. They seek to maintain consumer trust in their ability to protect a consumer's sensitive and personal information. The Marketplaces have standards for privacy and security of PII.

The Marketplace Privacy Policy at https://www.healthcare.gov/privacy/ provides consumers with information on how their personal information is used or shared and provides protections to prevent consumers from having their personal information used or shared in a harmful way or in a manner that is not authorized by federal law. Consumers will be informed about how their PII will be used.



Understanding Privacy Practices (con't)

The Department of Health and Human Services (HHS) oversees and monitors entities required to comply with Marketplace privacy and security standards, including assisters. HHS may conduct activities including, but not limited to: audits, investigations, inspections, and other activities related to oversight of compliance with Marketplace privacy and security standards. Civil, criminal, or administrative proceedings or actions may take place if there are unauthorized or inappropriate uses or disclosures of PII.

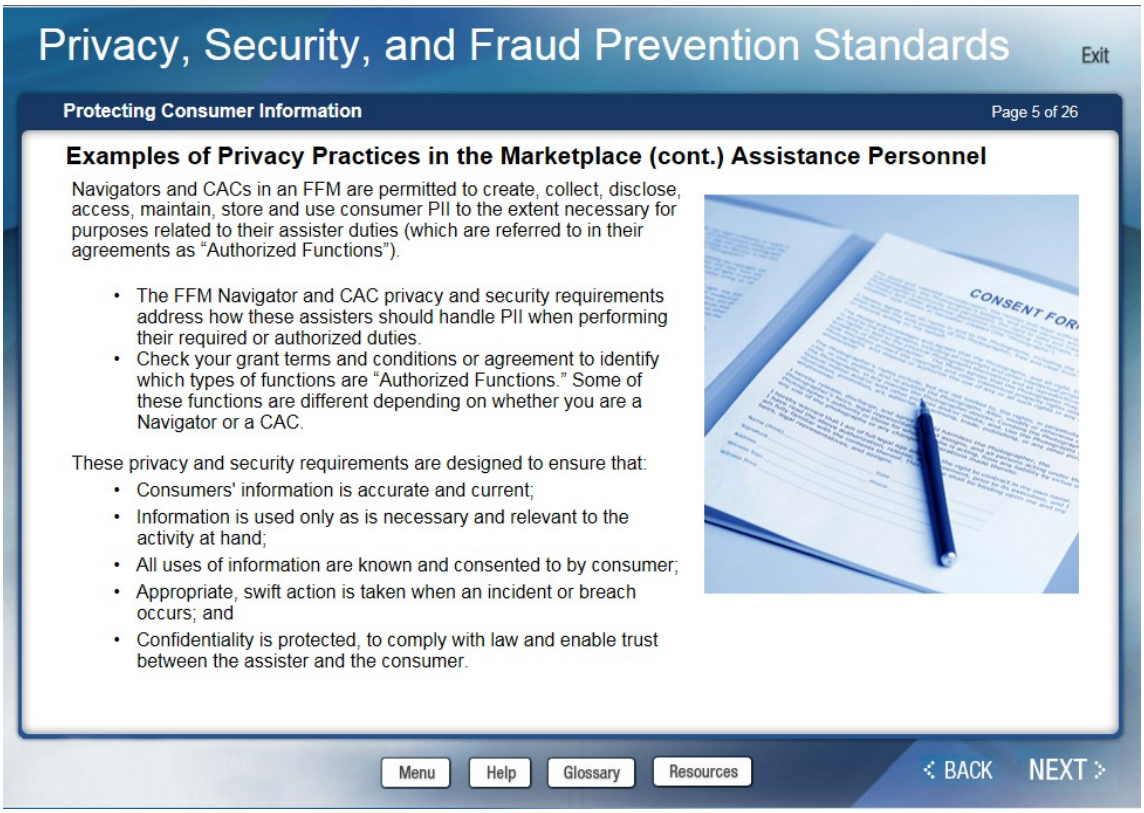
All Marketplaces, including the Federally Facilitated Marketplaces (FFMs), are required to have privacy and security standards (45 CFR §155.260(a)(3), (d)). The FFMs establish assister privacy and security standards through agreements with "non-Exchange entities," such as Navigator grantees and certified application counselor designated organizations.

Each Navigator and CAC organization in the FFM should refer to the privacy and security terms of its respective agreements.

Examples of these agreements include:

- Standard Grant/Cooperative Agreement Terms and Conditions for Navigator Grantees in the Federally-facilitated Marketplace and State Partnership Marketplaces
- CMS Certified Application Counselor Designated Organization Agreement

Individual CACs in an FFM should refer to the agreements they enter into with their CAC organizations, since these agreements must include the privacy and security standards established by the FFM.



Examples of Privacy Practices in the Marketplace (cont.) Assistance Personnel

Navigators and CACs in an FFM are permitted to create, collect, disclose, access, maintain, store and use consumer PII to the extent necessary for purposes related to their assister duties (which are referred to in their agreements as "Authorized Functions").

- The FFM Navigator and CAC privacy and security requirements address how these assisters should handle PII when performing their 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 are a Navigator or a CAC.

These privacy and security requirements are designed to ensure that:

- Consumers' information is accurate and current;
- Information is used only as is necessary and relevant to the activity at hand;
- All uses of information are known and consented to by consumer;
- Appropriate, swift action is taken when an incident or breach occurs; and
- Confidentiality is protected, to comply with law and enable trust between the assister and the consumer.

Examples of Privacy Practices in the Marketplace (cont) Assistance Personnel

Some examples of Marketplace privacy requirements are:

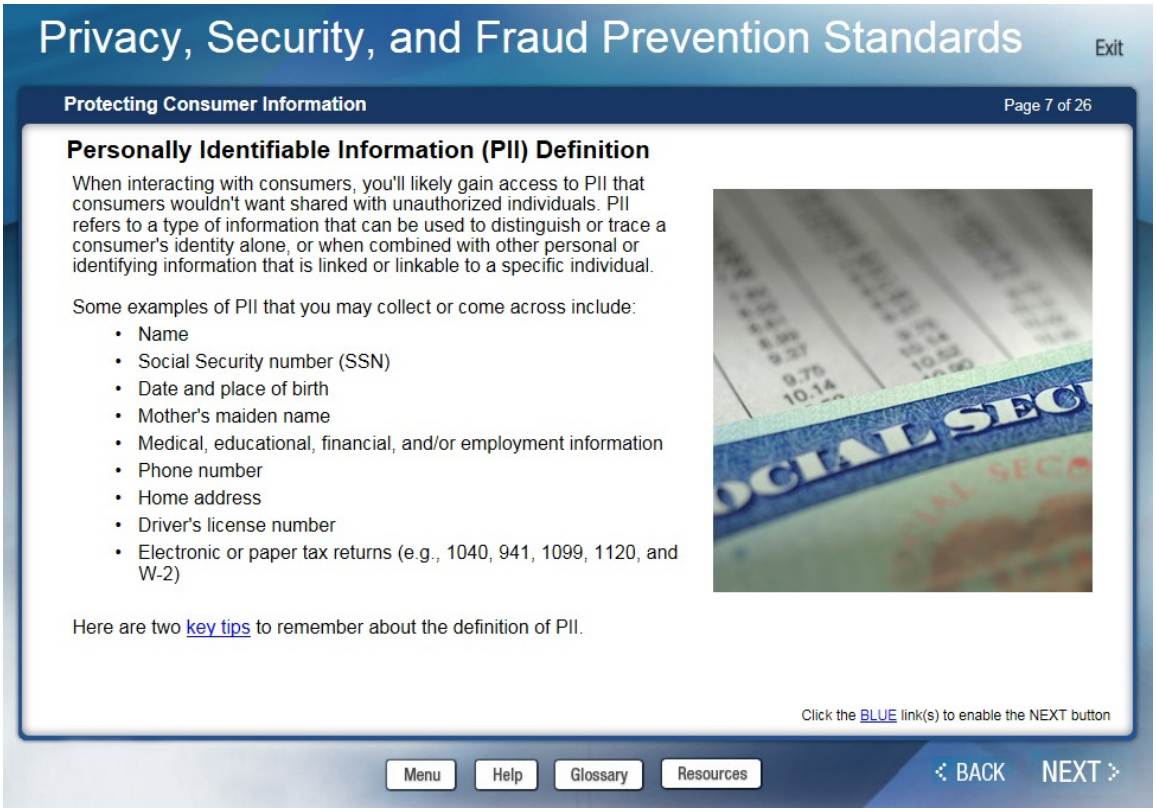
- Letting consumers know what personal information is collected by the assister, why it's collected, how it will be used, who the information can be shared with, and what happens if they don't want to provide the information
- Collecting only the information that's necessary to accomplish an authorized purpose
- Requiring you or your organization to obtain consent (or "authorization") from consumers indicating that they understand you will access the consumers' personal information to perform your duties as an assister
- Having policies and procedures for protecting and securing all personal information
- Following all applicable privacy and security requirements

This information is included in the privacy and security requirements that you or your organization received when you were approved to provide assistance to consumers. You must be familiar with these requirements to ensure that consumers' privacy is protected. Keep in mind that sub-grantees, or organizations with which you contract, are held to the

same standards as you regarding the use and disclosure of PII when assisting consumers with enrolling in coverage through the Marketplace.

More Information about Consent

Assisters are required to obtain consent from all consumers, orally or in writing, prior to obtaining access to a consumer's personal information, and keep a written record of that consent for at least six years under 45 Code of Federal Regulations (CFR) §155.210(e)(6)(ii), §155.215(g)(2), and §155.225(f)(2). The consent requirement will be covered later in this course.



Personally Identifiable Information (PII) Definition

When interacting with consumers, you'll likely gain access to PII that consumers wouldn't want shared with unauthorized individuals. PII refers to 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 linked or linkable to a specific individual.

Some examples of PII that you may collect or come across 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, 941, 1099, 1120, and W-2)

Here are two key tips to remember about the definition of PII.

Key Tip

Two key tips to remember about this definition are:

1. This definition may be different from definitions of PII under other laws. It's important that you're familiar with this specific federal definition and how it applies to Marketplace information.
2. A key part of the definition is that PII involves information which is linked or linkable to a specific individual. In other words, if it's possible to link information to a specific individual, this information would be considered PII, even if it hasn't been linked to that individual yet. Examples include, but aren't limited to, an individual's date of birth, place of birth, or mother's maiden name.

Prohibited Uses and Disclosures of PII

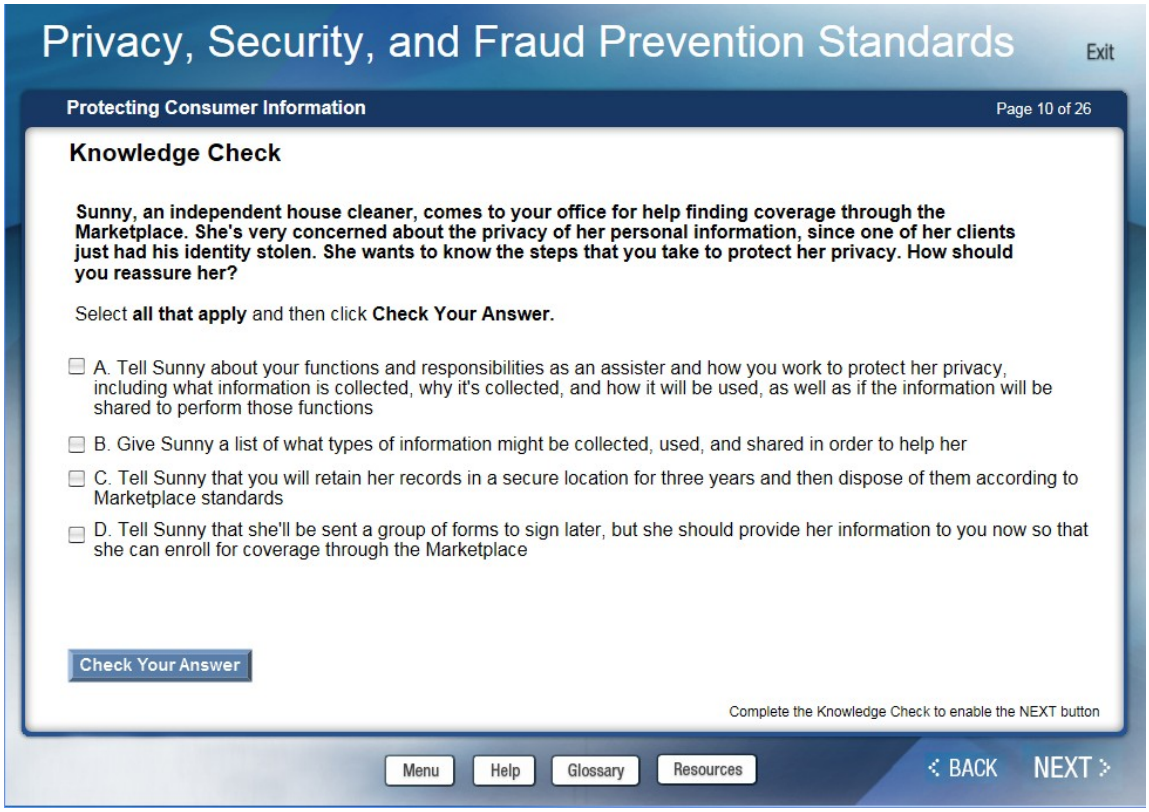
You must comply with the following restrictions on use of consumers' PII:

- You can't request information regarding citizenship, status as a national, or immigration status for any consumers who aren't seeking coverage for themselves on any application.
- You can't require any consumers who aren't seeking coverage for themselves to provide an SSN, unless information about the individual's income is necessary to determine the applicant's household income, or unless an individual's taxpayer identification number must be provided as part of a SHOP employer application under 45 CFR §155.730.
- (Note: an individual is not required to provide his or her SSN if he or she is not applying for coverage for himself or herself, but if the individual's income is included in the applicant's household income, providing this information can help speed up the verification process.)
- You can't collect PII beyond what is necessary to perform your authorized functions without the specific, informed consent of the consumer, or use PII to discriminate inappropriately against consumers, such as by refusing to assist individuals who are older or have significant or complex health care needs.

Instances When You May Come in Contact with PII

As you assist consumers applying for coverage through the Marketplace, you're likely to create, collect, disclose, access, maintain, store, and/or use PII when assisting consumers with, for example:

- Creating a Marketplace account
- Completing the eligibility process and submitting an application for health coverage
- Assessing options for lowering costs of health coverage
- Enrolling in a qualified health plan (QHP)



Knowledge Check

Sunny, an independent house cleaner, comes to your office for help finding coverage through the Marketplace. She's very concerned about the privacy of her personal information, since one of her clients just had his identity stolen. She wants to know the steps that you take to protect her privacy. How should you reassure her?

Select **all that apply**.

A. Tell Sunny about your functions and responsibilities as an assister and how you work to protect her privacy, including what information is collected, why it's collected, and how it will be used, as well as if the information will be shared to perform those functions

B. Give Sunny a list of what types of information might be collected, used, and shared in order to help her

C. Tell Sunny that you will retain her records in a secure location for three years and then dispose of them according to Marketplace standards

D. Tell Sunny that she'll be sent a group of forms to sign later, but she should provide her information to you now so that she can enroll for coverage through the Marketplace

Feedback: The correct answers are A and B. You should tell Sunny how you work to protect her privacy and explain to her what types of information might be collected, why it's collected, and how it will be used and shared in order for you to help her as an assister.

Assister Privacy and Security Standards

This section addresses Assister standards specifically.

Assisters must abide by their respective privacy and security standards to protect consumer information. The standards are supported by written grant terms and conditions (for Navigators), agreements (for CACs) or contracts (for Non-Navigator assistance personnel, i.e. Enrollment Assistance Program contractors) that should have been distributed to you or your organization when you were approved to provide assistance to consumers.

These standards include, but aren't limited to:

- Providing consumers with your organization's Privacy Notice Statement which explains your organization's privacy and security practices, as well as how to file complaints, prior to collecting consumer information for the purpose of performing your assister duties.
- Obtaining a consumer's consent (or authorization) either orally or in writing, prior to collecting, creating, disclosing, accessing, maintaining, storing, or using any consumer PII to perform an “Authorized Function,” which is a function that either relates to your assister duties or that is approved by CMS. A record of this consent must be stored for at least six years.

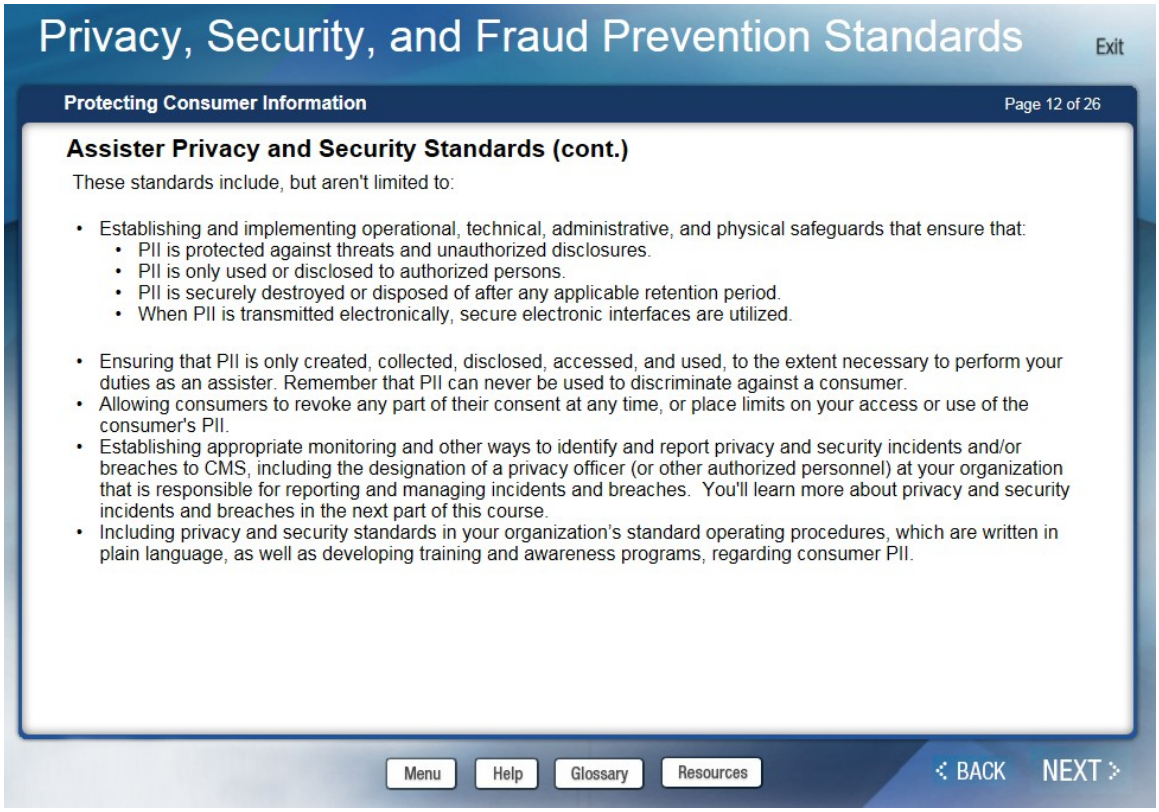
- If your organization intends to create, collect, disclose, access, maintain, store, or use consumer PII for any purpose that is NOT an Authorized Function, you and your organization must do the following:
    - Obtain specific informed consent from the consumer. A record of this consent must be stored for at least six years.
    - Maintain an accounting record of any disclosures of PII, including the date, nature, and purpose of the disclosure, name and address of the person or agency to whom the disclosure is made, and make this record available to a consumer upon request. This record must be retained for at least six years after the disclosure, or the life of the record, whichever is longer.

Privacy Notice Statement

Prior to collecting PII or other information from consumers for the purpose of performing your assister duties, you and/or your organization must provide a Privacy Notice Statement to consumers. If your organization maintains a website and will use that website to gather or request PII or other consumer information, the Privacy Notice Statement must also be prominently displayed on your organization's public-facing website. This Statement must be written in plain language and provided in a manner that is accessible and timely to people living with disabilities and with limited English proficiency. The Statement lets consumers know about important privacy issues such as what personal information is collected, why it's collected, how it'll be used, when the information can be shared, to whom the information will be shared, how the information will be kept secure, and how to file a privacy-related complaint with CMS and/or your organization.

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

Please note that the privacy and security standards do not require you and/or your organization to provide a Privacy Notice Statement every time you collect consumer information. Rather, you are permitted to collect basic contact information, such as a consumer's name, physical address, email address, or telephone number, without first providing a Privacy Notice Statement, if the sole purpose for collecting such contact information is to follow-up with a consumer to perform an “Authorized Function,” such as to schedule an appointment for application assistance, or to send a consumer educational or outreach information that is directly related to your assister duties.

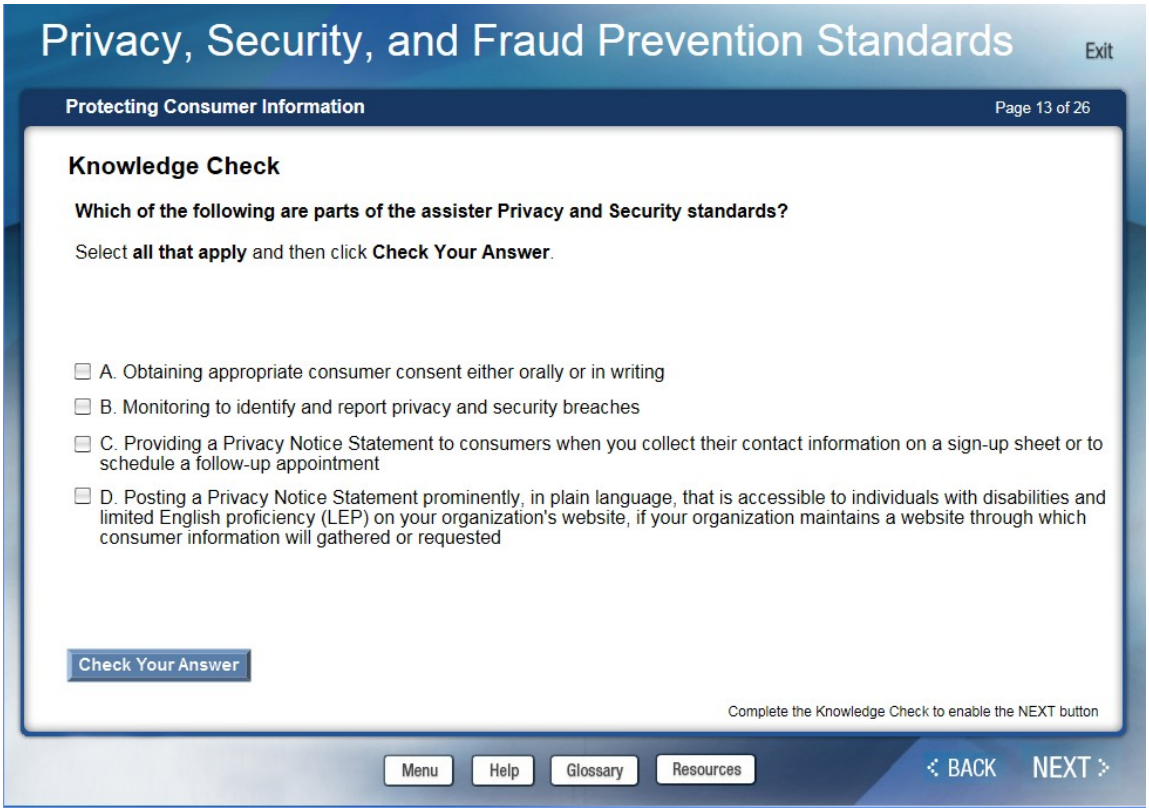


Assister Privacy and Security Standards (cont)

These standards include, but aren't limited to:

- Establishing and implementing operational, technical, administrative, and physical safeguards that ensure that:
    - PII is protected against threats and unauthorized disclosures.
    - PII is only used or disclosed to authorized persons.
    - PII is securely destroyed or disposed of after any applicable retention period.
    - When PII is transmitted electronically, secure electronic interfaces are utilized.
- Ensuring that PII is only created, collected, disclosed, accessed, and used, to the extent necessary to perform your duties as an assister. Remember that PII can never be used to discriminate against a consumer.
- Allowing consumers to revoke any part of their consent at any time, or place limits on your access or use of the consumer's PII.

- Establishing appropriate monitoring and other ways to identify and report privacy and security incidents and/or breaches to CMS, including the designation of a privacy officer (or other authorized personnel) at your organization that is responsible for reporting and managing incidents and breaches. You'll learn more about privacy and security incidents and breaches in the next part of this course.
- Including privacy and security standards in your organization's standard operating procedures, which are written in plain language, as well as developing training and awareness programs, regarding consumer PII.



Knowledge Check

Which of the following are parts of the assister Privacy and Security standards?

Select **all that apply.**

A. Obtaining appropriate consumer consent either orally or in writing

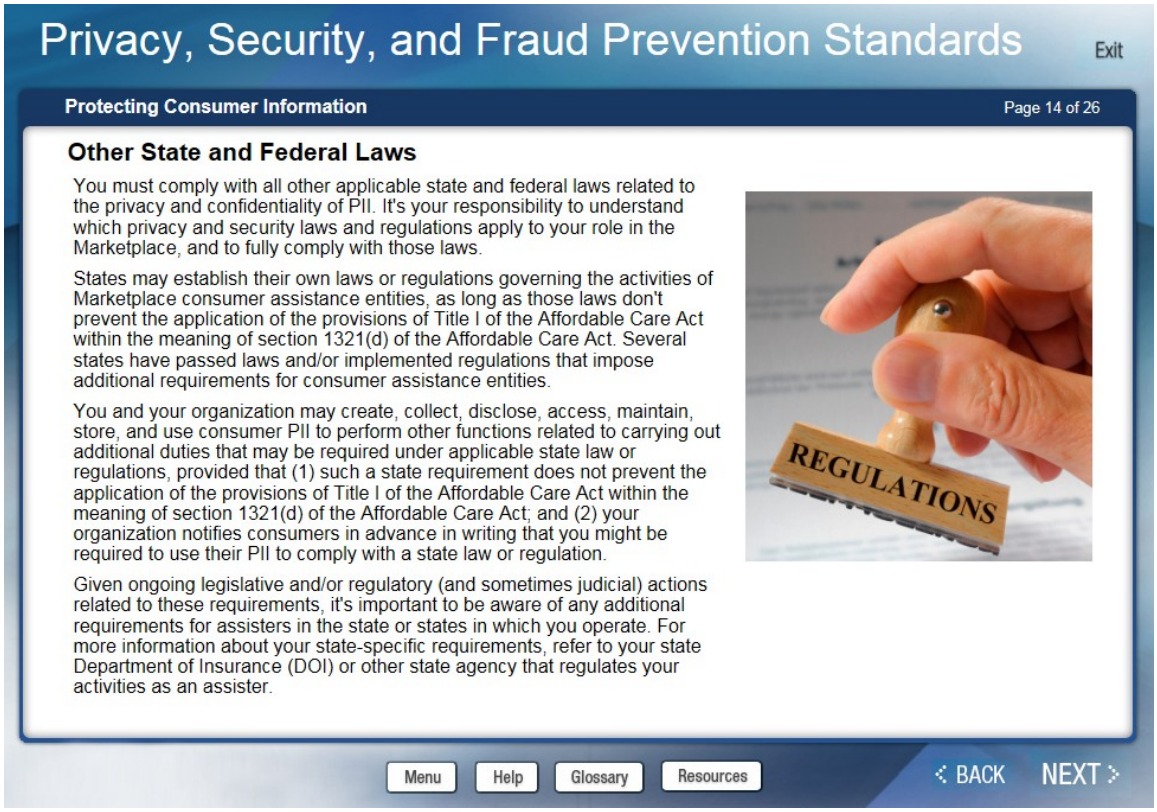
B. Monitoring to identify and report privacy and security breaches

C. Providing a Privacy Notice Statement to consumers when you collect their contact information on a sign-up sheet or to schedule a follow-up appointment

D. Posting a Privacy Notice Statement prominently, in plain language, that is accessible to individuals with disabilities and limited English proficiency (LEP) on your organization's website, if your organization maintains a website through which consumer information will gathered or requested.

Feedback: The correct answers are A, B and D. The Navigator and CAC Privacy and Security standards require you to obtain appropriate consumer consent orally or in writing, and require your organization to monitor for and report privacy and security breaches and to post its Privacy Notice Statement prominently, such as on any website it maintains through which consumer information will be gathered or requested. The standards don't require you to provide a Privacy Notice Statement every time you collect consumer information. Rather, you are permitted to collect basic contact information, such as a

consumer's name, physical address, email address, or telephone number, without first providing a Privacy Notice Statement, if the sole purpose for collecting such contact information is to follow-up with a consumer to perform an "Authorized Function," such as to schedule an appointment for application assistance, or to send a consumer educational or outreach information that is directly related to your assister duties.



Other State and Federal Laws

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 Marketplace, and to fully comply with those laws.

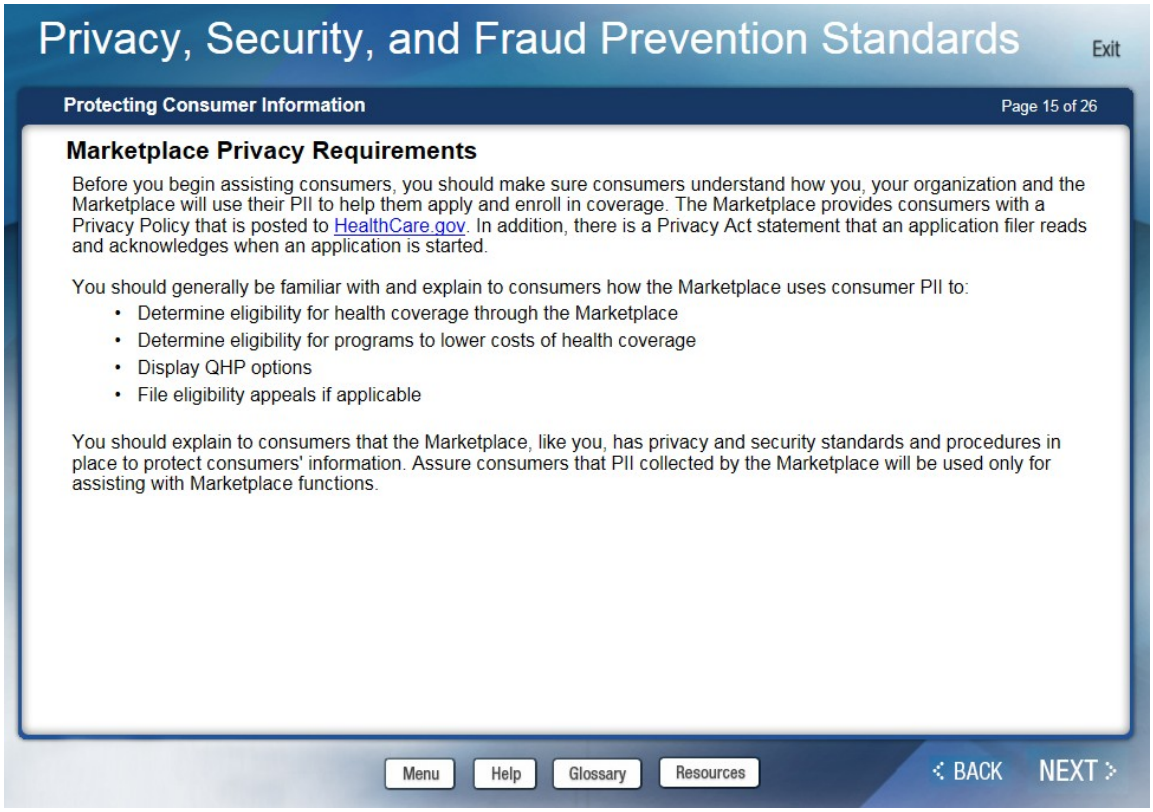
States may establish their own laws or regulations governing the activities of Marketplace consumer assistance entities, as long as those laws don't prevent the application of the provisions of Title I of the Affordable Care Act within the meaning of section 1321(d) of the Affordable Care Act. Several states have passed laws and/or implemented regulations that impose additional requirements for consumer assistance entities.

You and your organization may create, collect, disclose, access, maintain, store, and use consumer PII to perform other functions related to carrying out additional duties that may be required under applicable state law or regulations, provided that (1) such a state requirement does not prevent the application of the provisions of Title I of the Affordable Care Act within the meaning of section 1321(d) of the Affordable Care Act; and (2) your organization notifies 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 and/or regulatory (and sometimes judicial) actions related to these requirements, it's important to be aware of any additional requirements for

assisters in the state or states in which you 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.

Given ongoing legislative and/or regulatory (and sometimes judicial) actions related to these requirements, it's important to be aware of any additional requirements for assisters in the state or states in which you operate. For more information about your state-specific requirements, refer to your state Department of Insurance (DOI).



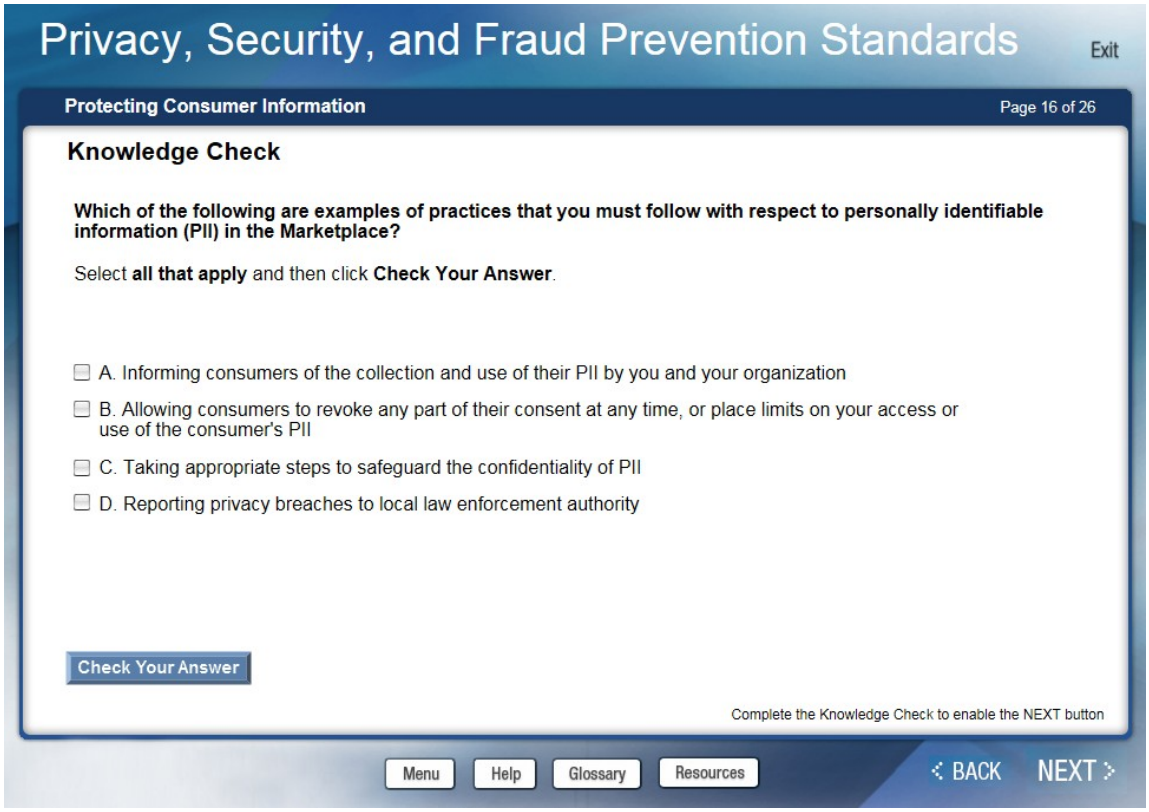
Marketplace Privacy Requirements

Before you begin assisting consumers, you should make sure consumers understand how you, your organization and the Marketplace will use their PII to help them apply and enroll in coverage. The Marketplace provides consumers with a Privacy Policy that is posted to HealthCare.gov. In addition, there is a Privacy Act statement that an application filer reads and acknowledges when an application is started.

You should generally be familiar with and explain to consumers how the Marketplace uses consumer PII to:

- Determine eligibility for health coverage through the Marketplace
- Determine eligibility for programs to lower costs of health coverage
- Display QHP options
- File eligibility appeals if applicable

You should explain to consumers that the Marketplace, like you, has privacy and security standards and procedures in place to protect consumers' information. Assure consumers that PII collected by the Marketplace will be used only for assisting with Marketplace functions.



Knowledge Check

Which of the following are examples of practices that you must follow with respect to personally identifiable information (PII) in the Marketplace?

Select **all that apply**.

A. Informing consumers of the collection and use of their PII by you and your organization

B. Allowing consumers to revoke any part of their consent at any time, or place limits on your access or use of the consumer's PII.

C. Taking appropriate steps to safeguard the confidentiality of PII

D. Reporting privacy breaches to local law enforcement authority

Feedback: The correct answers are A, B, and C. You must inform consumers of the collection and use of their PII by you and your organization by providing a Privacy Notice Statement to them, allow consumers to revoke any part of their consent at any time, or place limits on your access or use of the consumer's PII, and take appropriate steps to safeguard the confidentiality of PII. Privacy breaches shouldn't be reported to local law enforcement authorities, but to the Centers for Medicare & Medicaid Services (CMS) Information Technology (IT) Service Desk.

Obtain Consumer Consent

One of the first steps that you will take when providing application and enrollment assistance to a consumer for the first time will involve informing the consumer about your roles and responsibilities as an assister and obtaining that consumer's consent, which is sometimes referred to as getting the consumer's authorization. We use “consent” throughout this module for simplicity.

Ways to Obtain Consumer Consent

Consumers may give their consent themselves or choose to have a legal or authorized representative provide consent on their behalf, provided this is consistent with the scope of the representative's authority to act on the consumer's behalf. In addition, assisters may obtain a consumer's consent orally (such as over the phone), in writing, or both.

Consent forms should be in plain language and explained verbally by you to consumers before they sign (or orally consent). You should explain that by providing their consent consumers agree that you may have access to their PII in order to carry out your duties as an assister, such as helping them enroll in coverage through the Marketplace.

What the Consent Form Should Include

Consumer's Consent

At a minimum, a consumer's consent should include the following:

1. An acknowledgment that you informed the consumer of the functions and responsibilities that apply to your specific assister role (e.g., Navigator, CAC) (including all the consumer protection standards that apply through CMS regulations to your assister type, such as conflict of interest requirements, rules about accepting payment and providing gifts, etc.);
2. Consent for you to access and use the consumer's PII to carry out your Marketplace functions and responsibilities; and
3. An acknowledgment that the consumer may revoke any part of the consent at any time, as well as a description of any limitations that the consumer wants to place on your access or use of the consumer's PII.

Though not strictly required, we also recommend that the consent form include:

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 is not required to provide you with any PII;
3. An explanation that the help you provide is based only on the information the consumer provides, and that if the information given is inaccurate or incomplete, you might not be able to offer all the help that is available for the consumer's situation;
4. An acknowledgment that you will ask only for the minimum amount of PII necessary for you to carry out your functions and responsibilities; and
5. Any applicable specific consents to obtain access to consumer PII for CMS-approved purposes that are not already captured in the list of purposes set forth in your agreement with CMS.

Record of Consent

You must keep a record of the consumer’s consent. At a minimum, the record of the consent should include the following:

1. The consumer's name and (if applicable) the name of the legal or Marketplace authorized representative who provides consent on the consumer's behalf;
2. The date the consent form was given;
3. Your name, or the name of the assister to whom consent was given. Note that this could include additional names of assisters if the consumer authorized

multiple assisters within the same assister organization to obtain access to his or her PII;

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, including any applicable specific consents to access consumer PII for CMS-approved purposes that are not already captured in the list of purposes set forth in your agreement with CMS; and
6. If any changes are later made to the consent, including if and when a consumer revoked the consent, or any part thereof, this should be included with the original record.

Retention Period

In the Federally-facilitated Marketplaces, the minimum retention period for the record of the consumer's consent is no less than six years, unless a different and longer retention period has already been provided under other applicable Federal law.

If you are a Navigator or CAC, the Centers for Medicare & Medicaid Services (CMS) developed a model consent form that you or your organization may use as a guide. However, your organization is free to develop its own form and isn't required to use the CMS form.

Expiration

The regulations do not specify an automatic expiration date for the consumer's consent because it could become burdensome for a consumer consistently seeking services from the same assister to have to repeatedly renew the consent, and for the assister to have to maintain a record of each new consent for a minimum of six years. The regulations do not however, prevent assister organizations from setting an expiration date for consumer consents or requiring their periodic renewal. Unless the organization does so, the consent may last indefinitely if consistent with state law, unless the consumer revokes it. Under the CMS regulations, consumers are allowed to revoke their consent at any time, and may also place a time restriction on the consent at any time, if they desire.

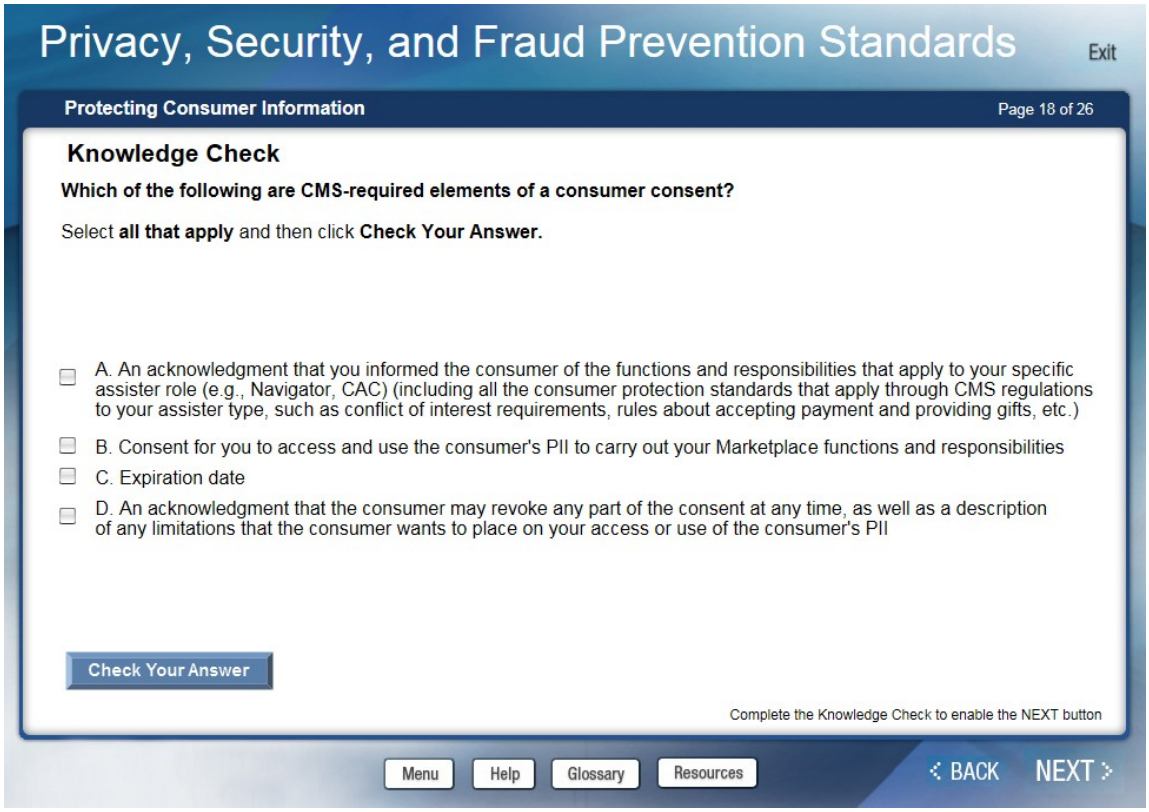
Obtaining Consumer Consent for Multiple Assisters within the Same Organization

It is not necessary for a consumer to provide a separate consent for each individual assister in an assister organization. We recognize that it could be burdensome to obtain a consumer's consent for each individual assister who is needed to assist with a particular consumer's access needs, Marketplace application, enrollment, or some other Marketplace coverage-related issue. To make it clearer that, generally speaking, the consumer's consent includes having any assister affiliated with a particular organization

access his or her PII if needed to carry out required assister duties, the CMS model consent forms have provided a clarification in the “general consent” section.

Please note that a consumer's ability to provide limitations or exceptions to his or her consent includes the ability to limit his or her consent to cover only assisters expressly identified on a consent form, or only assisters at a particular service location. Any such limitation or exception should be documented, and there is a space on the model forms to do so.

In addition, if a consumer seeks assistance from a different assister organization, even if it is for the same application or enrollment period, then the new assister or new assister organization, as applicable, must obtain a new consent from the consumer before assisting that consumer.



Knowledge Check

Which of the following are CMS-required elements of a consumer consent?

Select **all that apply**.

A. An acknowledgment that you informed the consumer of the functions and responsibilities that apply to your specific assister role (e.g., Navigator, CAC) (including all the consumer protection standards that apply through CMS regulations to your assister type, such as conflict of interest requirements, rules about accepting payment and providing gifts, etc.)

B. Consent for you to access and use the consumer's PII to carry out your Marketplace functions and responsibilities

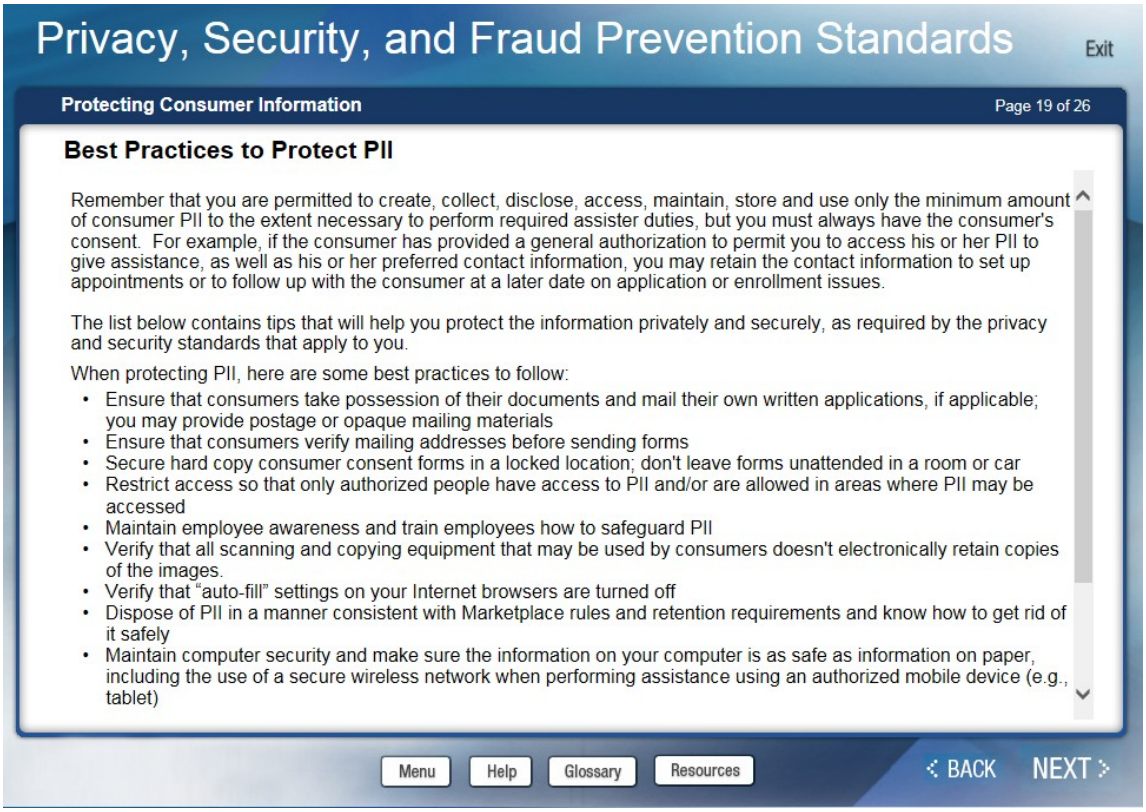
C. Expiration date

D. An acknowledgment that the consumer may revoke any part of the consent at any time, as well as a description of any limitations that the consumer wants to place on your access or use of the consumer's PII

Feedback: The correct answers are A, B, and D. The consent form must cover at least the following elements: an acknowledgment that you informed the consumer of the functions and responsibilities that apply to your specific assister role (e.g., Navigator, CAC) (including all the consumer protection standards that apply through CMS regulations to your assister

type, such as conflict of interest requirements, rules about accepting payment and providing gifts, etc.); consent for you to access and use the consumer's PII to carry out your Marketplace functions and responsibilities; and an acknowledgment that the consumer may revoke any part of the consent at any time, as well as a description of any limitations that the consumer wants to place on your access or use of the consumer's PII.

An expiration date isn't one of CMS's requirements for a consumer's consent but might be required by your state, and the consent can last indefinitely unless state law specifies otherwise. However, a consumer has the right to revoke the consent at any time and/or specify an expiration.



Best Practices to Protect PII

Remember that you are permitted to create, collect, disclose, access, maintain, store and use only the minimum amount of consumer PII to the extent necessary to perform required assister duties, but you must always have the consumer's consent. For example, if the consumer has provided a general authorization to permit you to access his or her PII to give assistance, as well as his or her preferred contact information, you may retain the contact information to set up appointments or to follow up with the consumer at a later date on application or enrollment issues.

The list below contains tips that will help you protect the information privately and securely, as required by the privacy and security standards that apply to you.

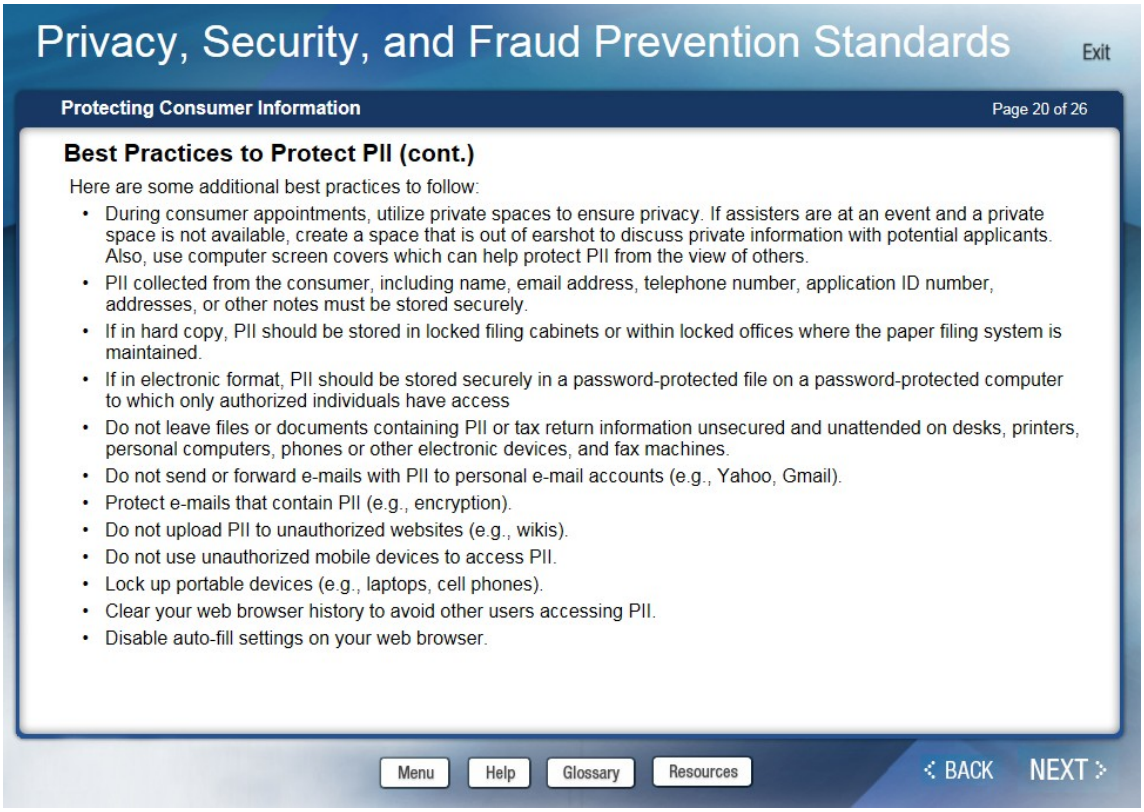
When protecting PII, here are some best practices to follow:

- Ensure that consumers take possession of their documents and mail their own written applications, if applicable; you may provide postage or opaque mailing materials
- Ensure that consumers verify mailing addresses before sending forms
- Secure hard copy consumer consent forms in a locked location; don't leave forms unattended in a room or car

- Restrict access so that only authorized people have access to PII and/or are allowed in areas where PII may be accessed
- Maintain employee awareness and train employees how to safeguard PII
- Verify that all scanning and copying equipment that may be used by consumers doesn't electronically retain copies of the images.
- Verify that “auto-fill” settings on your Internet browsers are turned off
- Dispose of PII in a manner consistent with Marketplace rules and retention requirements and know how to get rid of it safely
- Maintain computer security and make sure the information on your computer is as safe as information on paper, including the use of a secure wireless network when performing assistance using an authorized mobile device (e.g., tablet)

Always ensure that any hard copies of consumers' records are returned prior to them departing your facility and only make copies for yourself or others if necessary to carry out required duties. It can be helpful to have a supply of manila folders to hand to consumers with their documents inside, to keep their documents in one place and shield the content from view.

If PII is left with you by accident, store the documents in a safe, locked location, and return PII to consumers as soon as possible. Be sure to follow the procedures of the Marketplace and your organization for this issue.

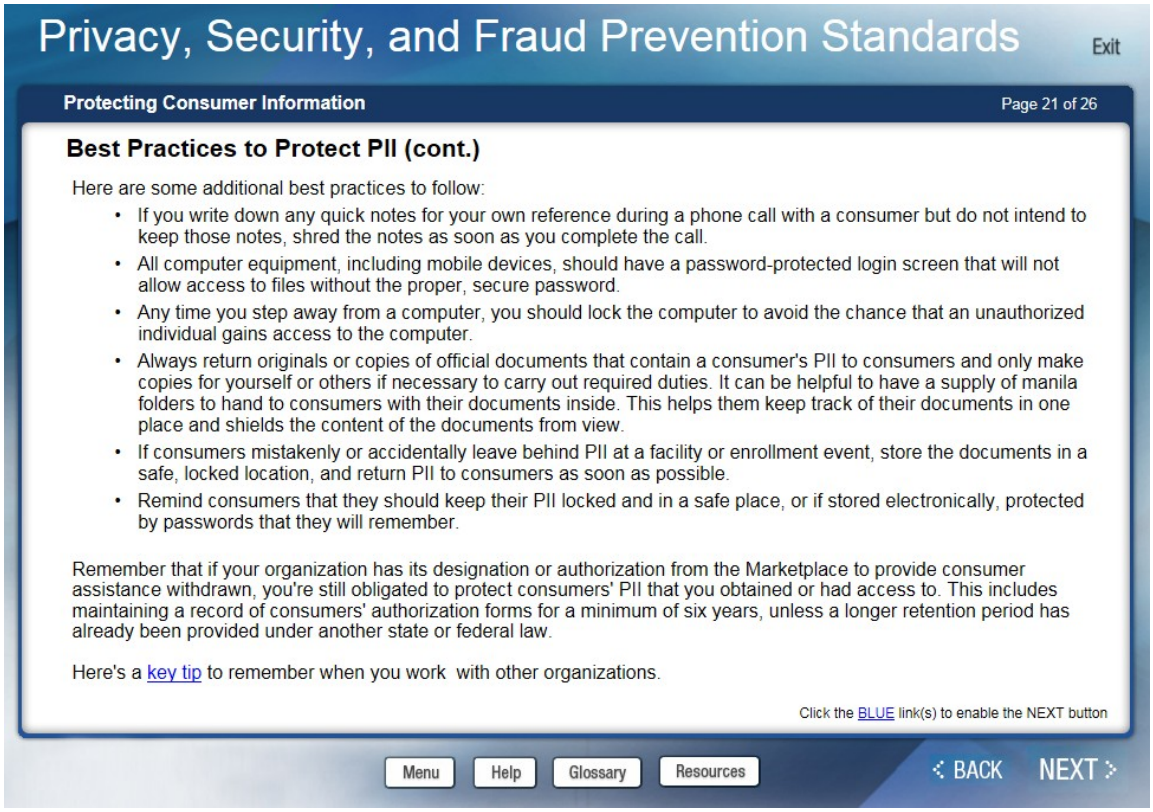


Best Practices to Protect PII (cont)

Here are some additional best practices to follow:

- During consumer appointments, utilize private spaces to ensure privacy. If assisters are at an event and a private space is not available, create a space that is out of earshot to discuss private information with potential applicants. Also, use computer screen covers which can help protect PII from the view of others.
- PII collected from the consumer, including name, email address, telephone number, application ID number, addresses, or other notes must be stored securely.
- If in hard copy, PII should be stored in locked filing cabinets or within locked offices where the paper filing system is maintained.
- 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
- Do not leave files or documents containing PII or tax return information unsecured and unattended on desks, printers, personal computers, phones or other electronic devices, and fax machines.

- Do not send or forward e-mails with PII to personal e-mail accounts (e.g., Yahoo, Gmail).
- Protect e-mails that contain PII (e.g., encryption).
- Do not upload PII to unauthorized websites (e.g., wikis).
- Do not use unauthorized mobile devices to access PII.
- Lock up portable devices (e.g., laptops, cell phones).
- Clear your web browser history to avoid other users accessing PII.
- Disable auto-fill settings on your web browser.



Best Practices to Protect PII (cont)

Here are some additional best practices to follow:

- If you write down any quick notes for your own reference during a phone call with a consumer but do not intend to keep those notes, shred the notes as soon as you complete the call.
- All computer equipment, including mobile devices, should have a password-protected login screen that will not allow access to files without the proper, secure password.
- Any time you step away from a computer, you should lock the computer to avoid the chance that an unauthorized individual gains access to the computer.
- Always return originals or copies of official documents that contain a consumer's PII to consumers and only make copies for yourself or others if necessary to carry out required duties. It can be helpful to have a supply of manila folders to hand to consumers with their documents inside. This helps them keep track of their documents in one place and shields the content of the documents from view.
- If consumers mistakenly or accidentally leave behind PII at a facility or enrollment event, store the documents in a safe, locked location, and return PII to consumers as soon as possible.

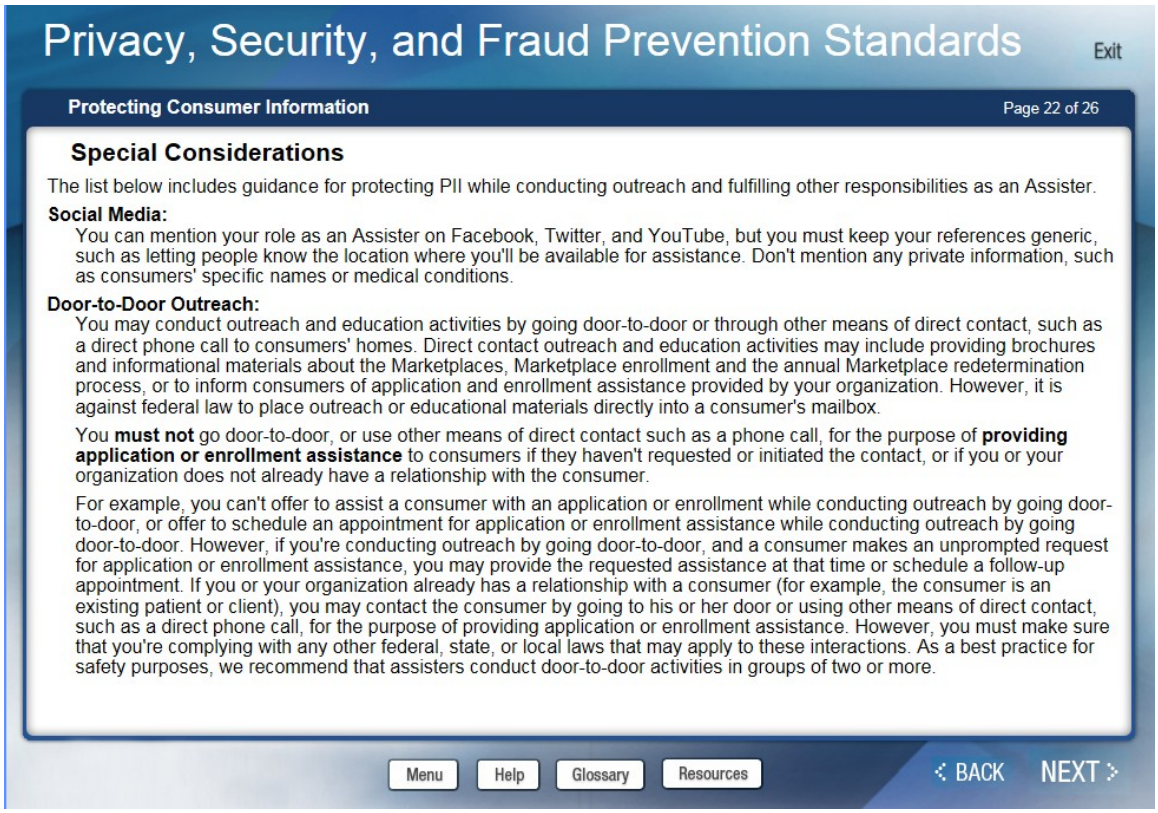
- Remind consumers that they should keep their PII locked and in a safe place, or if stored electronically, protected by passwords that they will remember.

Remember that if your organization has its designation or authorization from the Marketplace to provide consumer assistance withdrawn, you're still obligated to protect consumers' PII that you obtained or had access to. This includes maintaining a record of consumers' authorization forms for a minimum of six years, unless a longer retention period has already been provided under another state or federal law.

Here's a key tip to remember when you work with other organizations.

Key Tip

In addition, if you work with other organizations in your work with the Marketplace, you remain legally bound and responsible for all obligations to protect consumers' PII and are required to obligate the other organization to the same privacy and security standards to which you are bound.



Special Considerations

The list below includes guidance for protecting PII while conducting outreach and fulfilling other responsibilities as an Assister.

Social Media

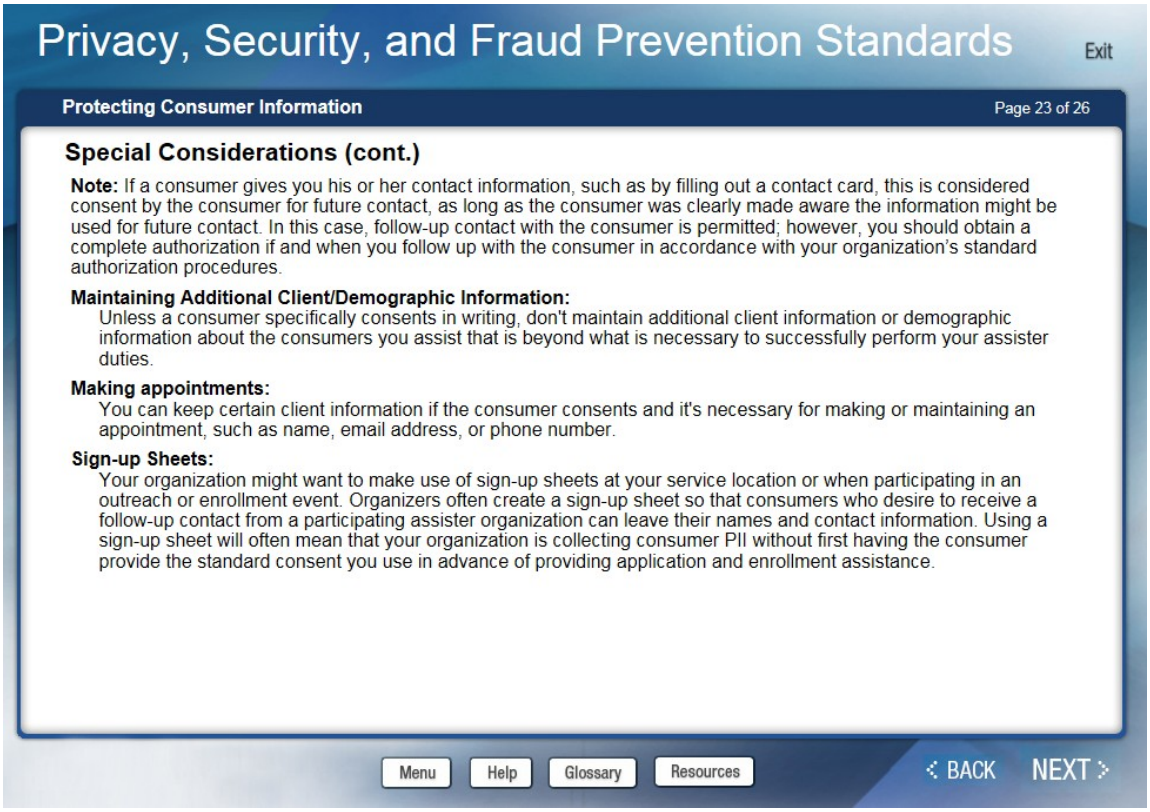
You can mention your role as an Assister on Facebook, Twitter, and YouTube, but you must keep your references generic, such as letting people know the location where you'll be available for assistance. Don't mention any private information, such as consumers' specific names or medical conditions.

Door-to-Door Outreach

You may conduct outreach and education activities by going door-to-door or through other means of direct contact, such as a direct phone call to consumers' homes. Direct contact outreach and education activities may include providing brochures and informational materials about the Marketplaces, Marketplace enrollment and the annual Marketplace redetermination process, or to inform consumers of application and enrollment assistance provided by your organization. However, it is against federal law to place outreach or educational materials directly into a consumer's mailbox.

You **must not** go door-to-door, or use other means of direct contact such as a phone call, for the purpose of **providing application or enrollment assistance** to consumers if they haven't requested or initiated the contact, or if you or your organization does not already have a relationship with the consumer.

For example, you can't offer to assist 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, if you're conducting outreach by going door-to-door, and a consumer makes an unprompted request for application or enrollment assistance, you may provide the requested assistance at that time or schedule a follow-up appointment. If you or your organization already has a relationship with a consumer (for example, the consumer is an existing patient or client), you may contact the consumer by going to his or her door or using other means of direct contact, such as a direct phone call, for the purpose of providing application or enrollment assistance. However, you must make sure that you're complying with any other federal, state, or local laws that may apply to these interactions. As a best practice for safety purposes, we recommend that assisters conduct door-to-door activities in groups of two or more.



Special Considerations (cont)

Note: If a consumer gives you his or her contact information, such as by filling out a contact card, this is considered consent by the consumer for future contact, as long as the consumer was clearly made aware the information might be used for future contact. In this case, follow-up contact with the consumer is permitted; however, you should obtain a complete authorization if and when you follow up with the consumer in accordance with your organization's standard authorization procedures.

Maintaining Additional Client/Demographic Information

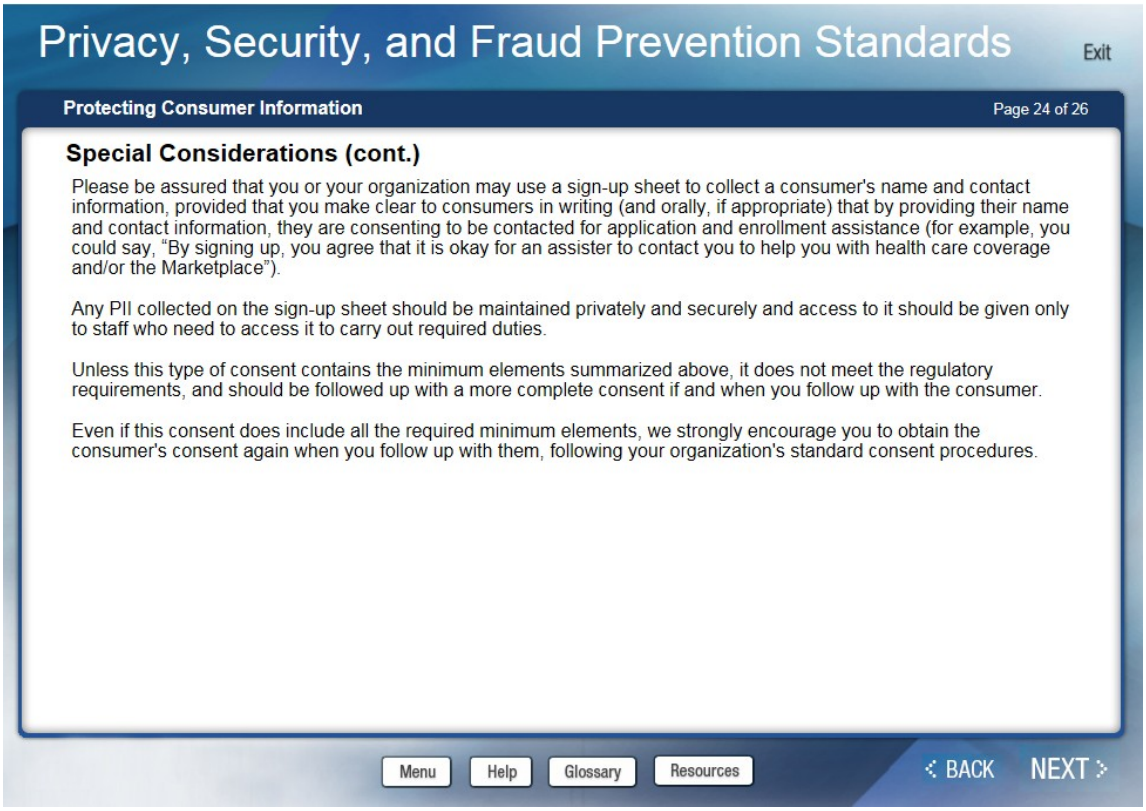
Unless a consumer specifically consents in writing, don't maintain additional client information or demographic information about the consumers you assist that is beyond what is necessary to successfully perform your assister duties.

Making appointments

You can keep certain client information if the consumer consents and it's necessary for making or maintaining an appointment, such as name, email address, or phone number.

Sign-up Sheets

Your organization might want to make use of sign-up sheets at your service location or when participating in an outreach or enrollment event. Organizers often create a sign-up sheet so that consumers who desire to receive a follow-up contact from a participating assister organization can leave their names and contact information. Using a sign-up sheet will often mean that your organization is collecting consumer PII without first having the consumer provide the standard consent you use in advance of providing application and enrollment assistance.



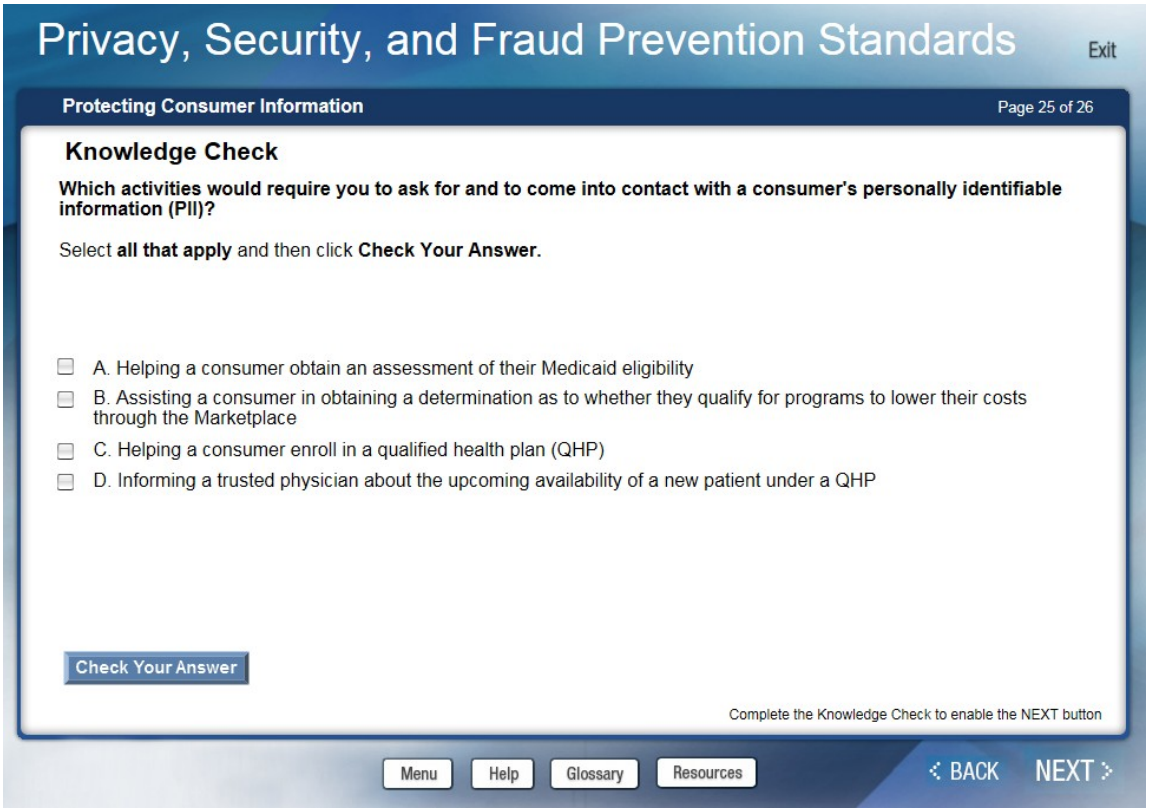
Special Considerations (cont)

Please be assured that you or your organization may use a sign-up sheet to collect a consumer's name and contact information, provided that you make clear to consumers in writing (and orally, if appropriate) that by providing their name and contact information, they are consenting to be contacted for application and enrollment assistance (for example, you could say, "By signing up, you agree that it is okay for an assister to contact you to help you with health care coverage and/or the Marketplace").

Any PII collected on the sign-up sheet should be maintained privately and securely and access to it should be given only to staff who need to access it to carry out required duties.

Unless this type of consent contains the minimum elements summarized above, it does not meet the regulatory requirements, and should be followed up with a more complete consent if and when you follow up with the consumer.

Even if this consent does include all the required minimum elements, we strongly encourage you to obtain the consumer's consent again when you follow up with them, following your organization's standard consent procedures.



Knowledge Check

Which activities would require you to ask for and to come into contact with a consumer's personally identifiable information (PII)?

Select **all that apply**.

A. Helping a consumer obtain an assessment of their Medicaid eligibility

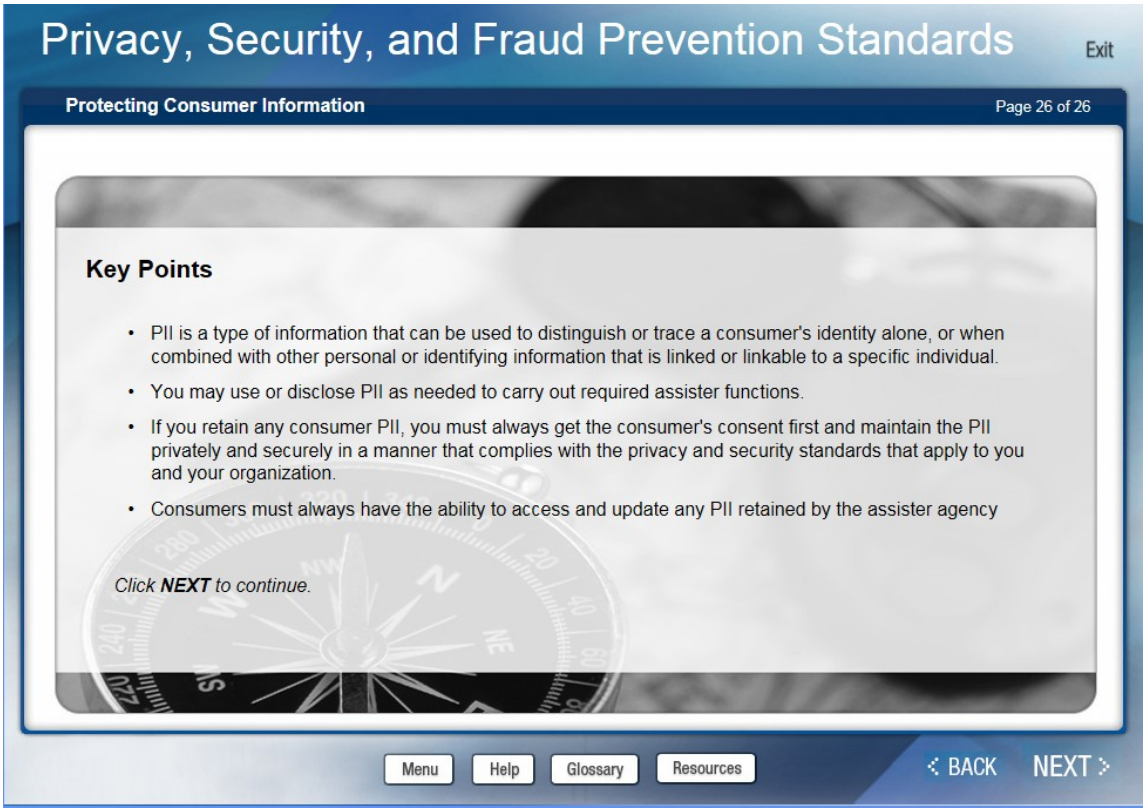
B. Assisting a consumer in obtaining a determination as to whether they qualify for programs to lower their costs through the Marketplace

C. Helping a consumer enroll in a qualified health plan (QHP)

D. Informing a trusted physician about the upcoming availability of a new patient under a QHP

Feedback: The correct answers are A, B, and C. You may come into contact with and use PII, such as information about a consumer's residency or income, while helping a consumer obtain an assessment of their Medicaid eligibility, while assisting a consumer in determining whether they qualify for programs to lower their costs, and while helping a consumer enroll in a QHP. Remember that you should only use the PII to the extent necessary to accomplish a specific purpose under the Marketplace. You may use PII for another lawful purpose, but you must obtain a consumer's specific consent first, and that

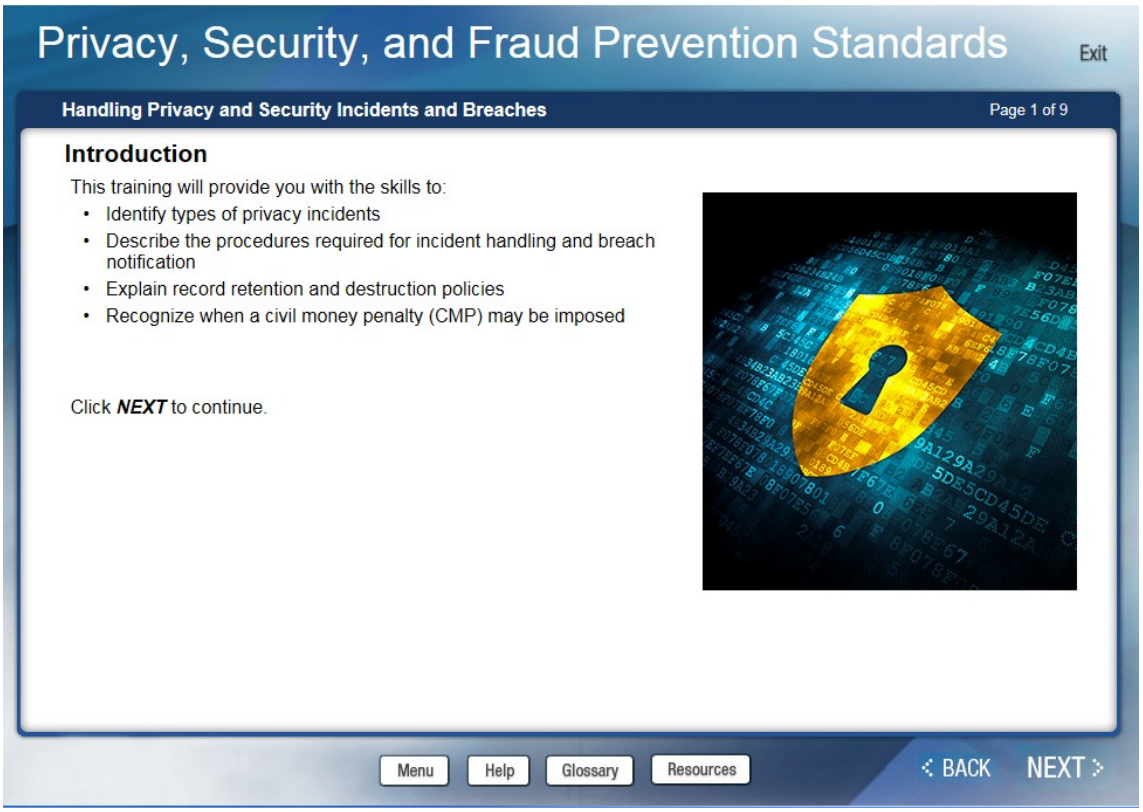
consent must be maintained separate from the consent you use to perform your assister duties.



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 linked or linkable to a specific individual.
- You may use or disclose PII as needed to carry out required assister functions.
- If you retain any consumer PII, you must always get the consumer's consent first and maintain the PII privately and securely in a manner that complies with the privacy and security standards that apply to you and your organization.
- Consumers must always have the ability to access and update any PII retained by the assister agency

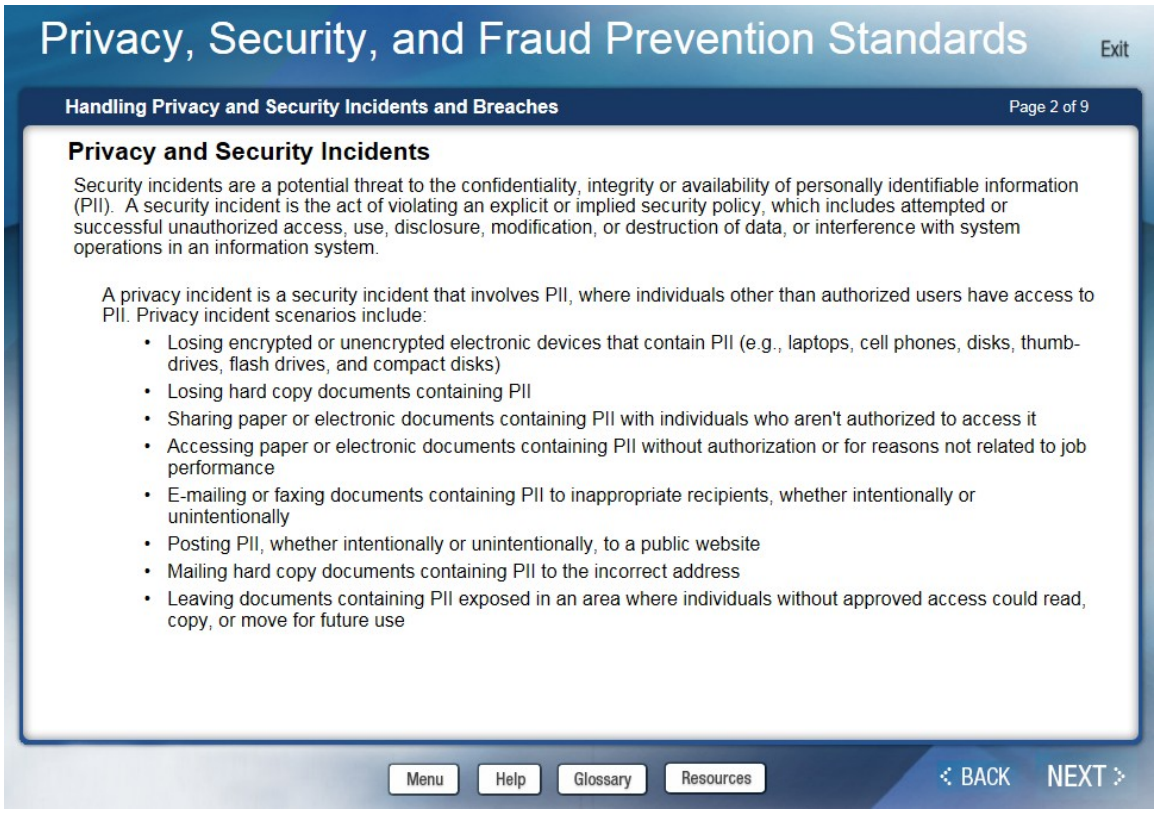
Handling Privacy and Security Incidents and Breaches Module



Introduction

This training will provide you with the skills to:

- Identify types of privacy incidents
- Describe the procedures required for incident handling and breach notification
- Explain record retention and destruction policies
- Recognize when a civil money penalty (CMP) may be imposed



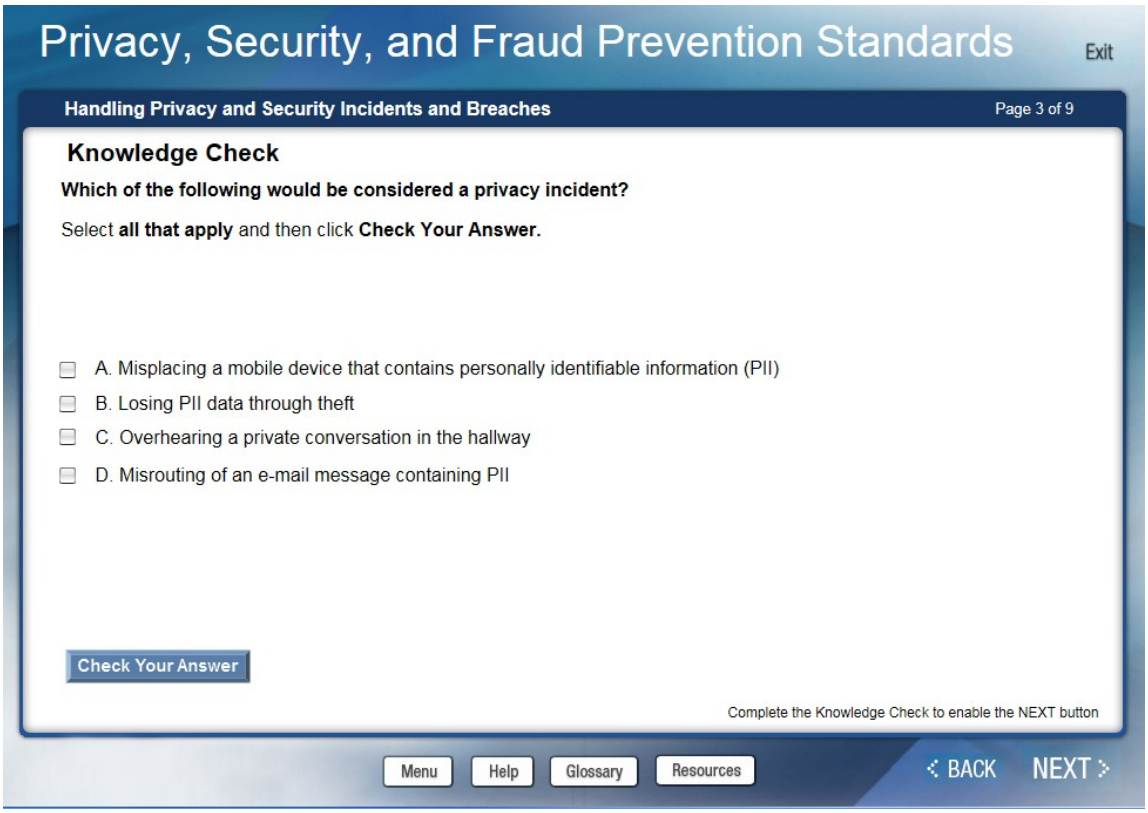
Privacy and Security Incidents

Security incidents are a potential threat to the confidentiality, integrity or availability of personally identifiable information (PII). A security incident is the act 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 that involves PII, where individuals other than authorized users have access to PII. Privacy incident scenarios include:

- Losing encrypted or unencrypted electronic devices that contain PII (e.g., laptops, cell phones, disks, thumb-drives, flash drives, and compact disks)
- 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
- E-mailing or faxing documents containing PII to inappropriate recipients, whether intentionally or unintentionally

- Posting PII, whether intentionally or unintentionally, to a public website
- Mailing hard copy documents containing PII to the incorrect address
- Leaving documents containing PII exposed in an area where individuals without approved access could read, copy, or move for future use



Knowledge Check

Which of the following would be considered a privacy incident?

Select **all that apply**.

A. Misplacing a mobile device that contains personally identifiable information (PII)

B. Losing PII data through theft

C. Overhearing a private conversation in the hallway

D. Misrouting of an e-mail message containing PII

Feedback: The correct answers are A, B, and D. 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 the 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 seeing or possessing the information or losing the records, the incident should be reported to CMS within one hour of discovery.

As an organization approved to provide assistance to consumers, your organization should have written procedures in place for addressing privacy and security issues.

File a Breach Report

Assister organizations must implement breach and incident handling procedures that are consistent with CMS' Risk Management Handbook Standard 7.1 Incident Handling and Breach Notification, and which include details regarding 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 (such as a Privacy Official or Officer) who are responsible for reporting and managing Incidents or Breaches to CMS.

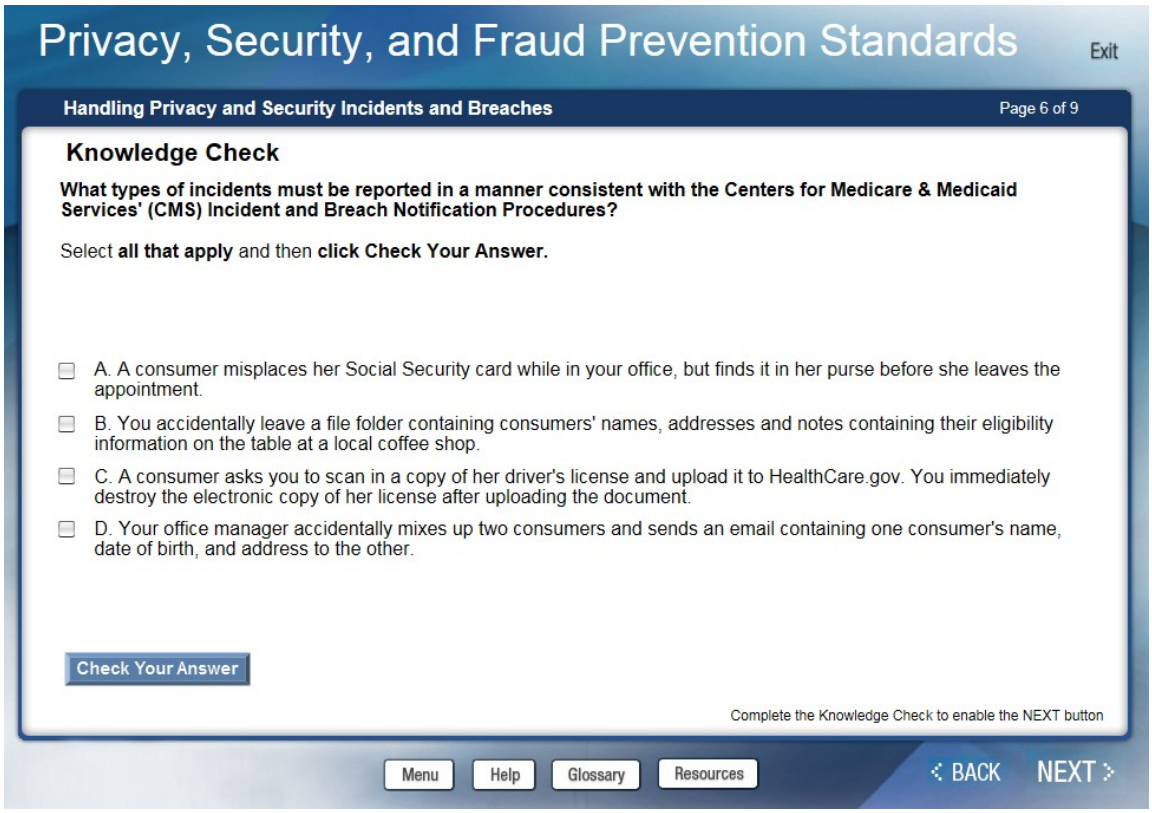
Procedures must require reporting of any incident or breach of PII to the CMS Information Technology (IT) Help Desk by telephone at:

- **(410) 786-2580** or
- **(800) 562-1963** or
- via e-mail notification within required time frames at: **cms_it_service_desk@cms.hhs.gov**

Issues you should report include:

- Lost, stolen, or misplaced records or computers
- Unauthorized personnel or other third parties seeing or possessing PII information

- Instances you recognize as having the potential to compromise consumer information



Knowledge Check

What types of incidents must be reported in a manner consistent with the Centers for Medicare & Medicaid Services' (CMS) Incident and Breach Notification Procedures?

Select **all that apply**.

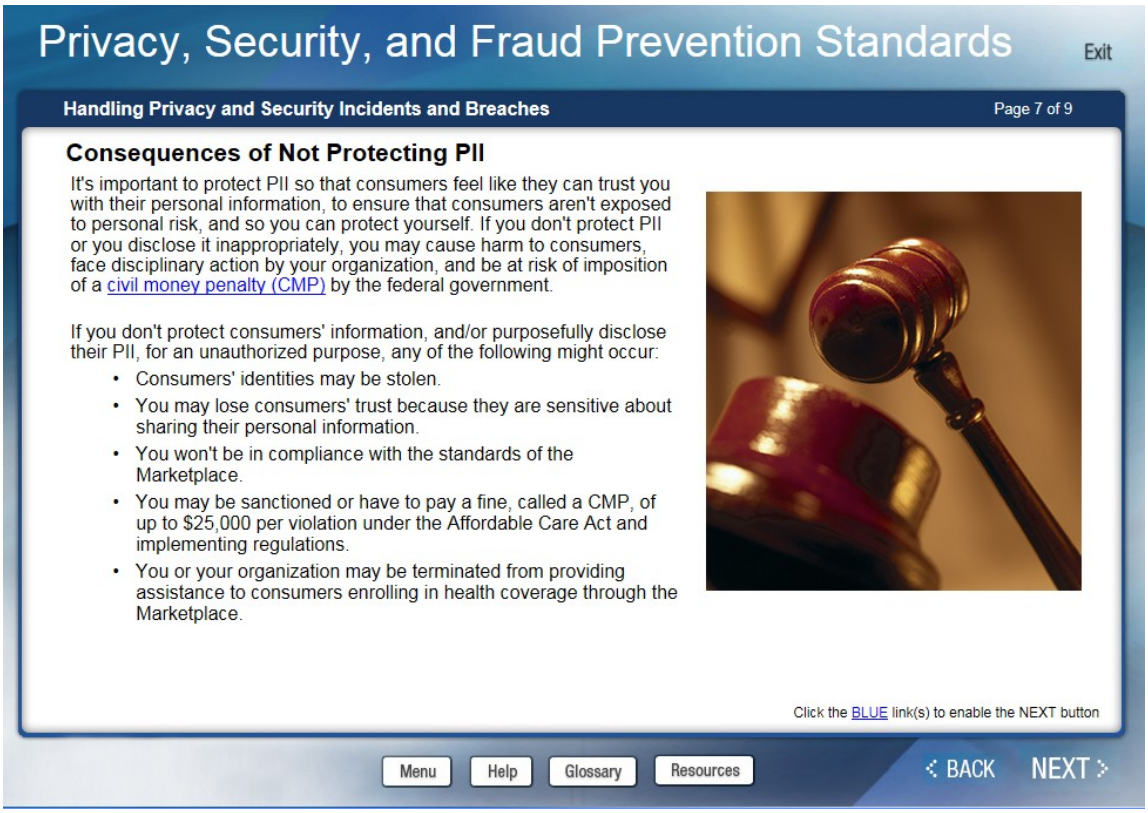
A. A consumer misplaces her Social Security card while in your office, but finds it in her purse before she leaves the appointment.

B. You accidentally leave a file folder containing consumers' names, addresses and notes containing their eligibility information on the table at a local coffee shop.

C. A consumer asks you to scan in a copy of her driver's license and upload it to HealthCare.gov. You immediately destroy the electronic copy of her license after uploading the document.

D. Your office manager accidentally mixes up two consumers and sends an email containing one consumer's name, date of birth, and address to the other.

Feedback: The correct answers are B and D. If you accidentally leave a file folder containing personally identifiable information (PII) in a public location or your office manager shares information from one consumer with another person without his or her consent, you could be putting your consumers at risk of identity theft or otherwise having their privacy violated.



Consequences of Not Protecting PII

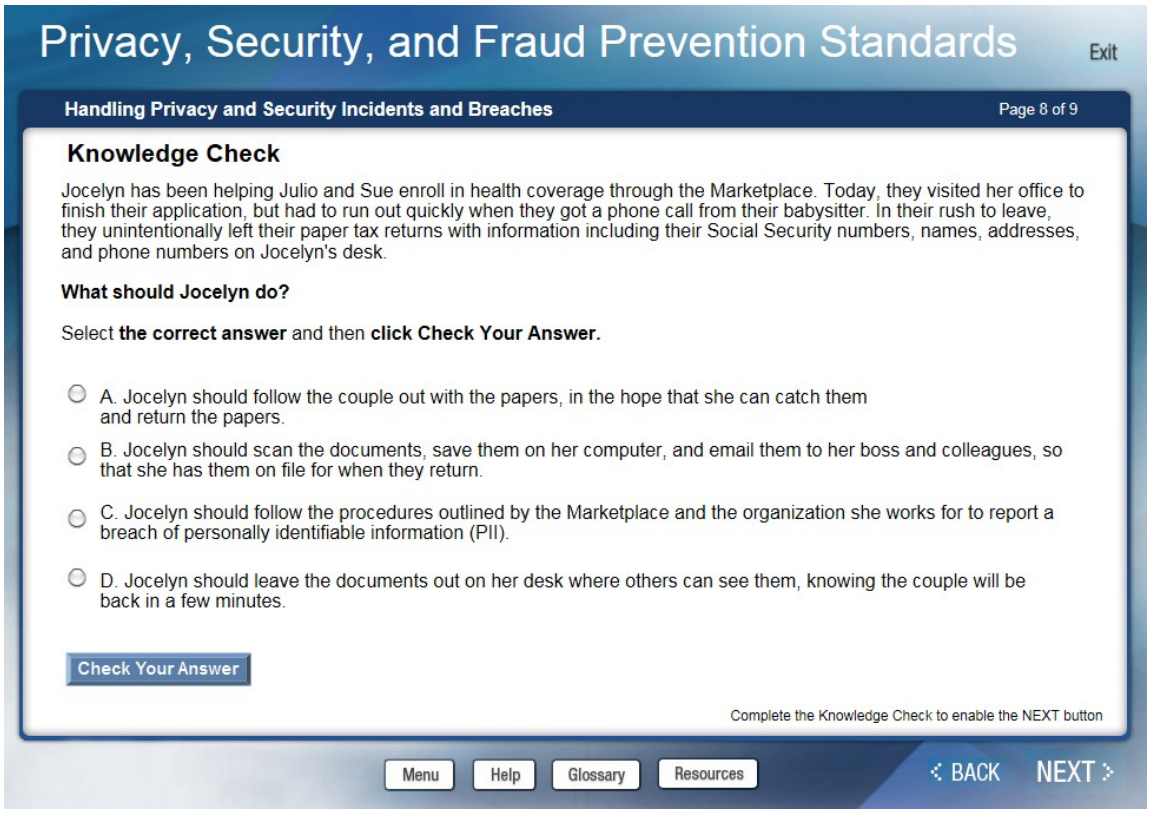
It's important to protect PII so that consumers feel like they can trust you with their personal information, to ensure that consumers aren't exposed to personal risk, and so you can protect yourself. If you don't protect PII or you disclose it inappropriately, you may cause harm to consumers, face disciplinary action by your organization, and be at risk of imposition of a civil money penalty (CMP) by the federal government.

If you don't 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 in compliance with the standards of the Marketplace.
- You may be sanctioned or have to pay a fine, called a CMP, of up to $25,000 per violation under the Affordable Care Act and implementing regulations.
- You or your organization may be terminated from providing assistance to consumers enrolling in health coverage through the Marketplace.

More Information about the Civil Money Penalty

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



Knowledge Check

Jocelyn has been helping Julio and Sue enroll in health coverage through the Marketplace. Today, they visited her office to finish their application, but had to run out quickly when they got a phone call from their babysitter. In their rush to leave, they unintentionally left their paper tax returns with information including their Social Security numbers, names, addresses, and phone numbers on Jocelyn's desk.

What should Jocelyn do?

Select **the correct answer.**

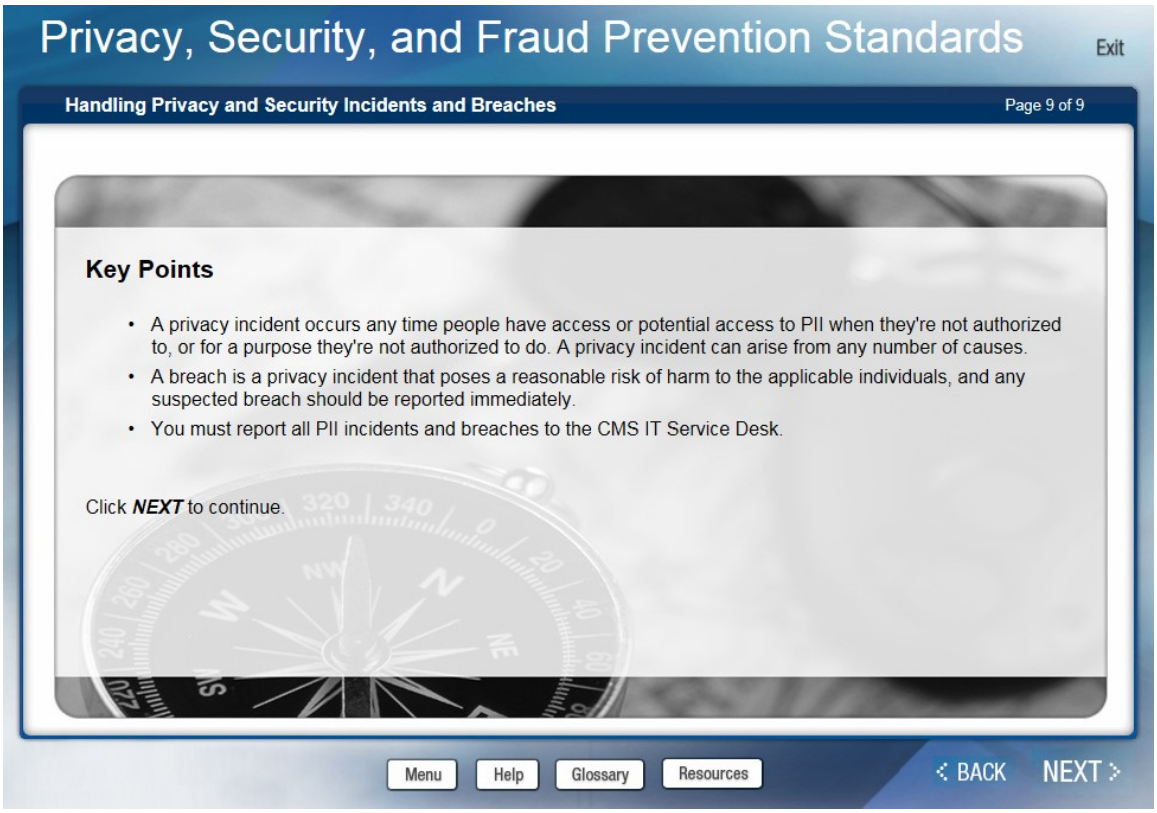
A. Jocelyn should follow the couple out with the papers, in the hope that she can catch them and return the papers.

B. Jocelyn should scan the documents, save them on her computer, and email them to her boss and colleagues, so that she has them on file for when they return.

C. Jocelyn should follow the procedures outlined by the Marketplace and the organization she works for to report a breach of personally identifiable information (PII).

D. Jocelyn should leave the documents out on her desk where others can see them, knowing the couple will be back in a few minutes.

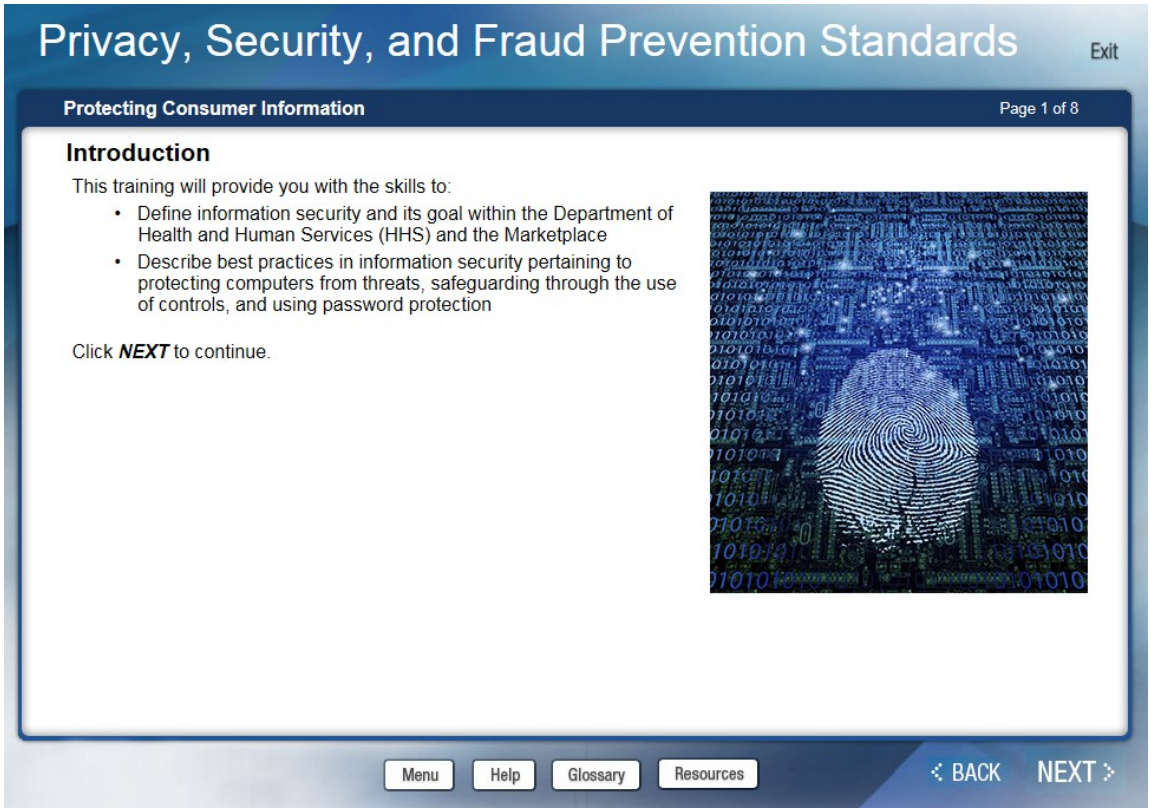
Feedback: The correct answer is A. Jocelyn should follow the couple out with the papers, in the hope that she can catch them and return the papers. In case she is unable to find them, she should attempt to contact them to ask that they retrieve their papers. In the meantime, the papers should be kept private and secure.



Key Points

- A privacy incident occurs any time people have access or potential access to PII when they're not authorized to, or for a purpose they're not authorized to do. A privacy incident can arise from any number of causes.
- A breach is a privacy incident that poses a reasonable risk of harm to the applicable individuals, and any suspected breach should be reported immediately.
- You must report all PII incidents and breaches to the CMS IT Service Desk.

Protecting Consumer Information Module



Introduction

This training will provide you with the skills to:

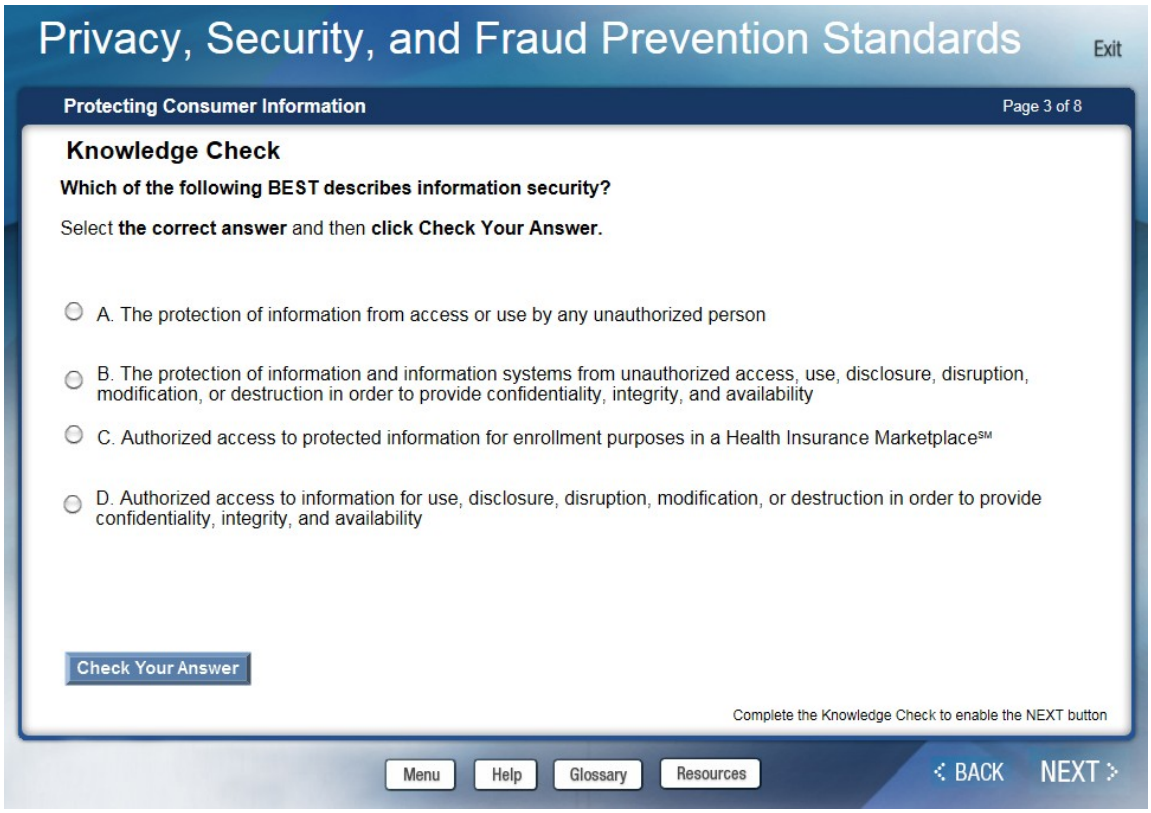
- Define information security and its goal within the Department of Health and Human Services (HHS) and the Marketplace
- Describe best practices in information security pertaining to protecting computers from threats, safeguarding through the use of controls, and using password protection

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, in order 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, HHS has a media neutral policy towards information. This means that any data must be protected — whether it is in electronic, paper, or oral format.



Knowledge Check

Which of the following BEST describes information security?

Select **the correct answer**.

A. The protection of information from access or use by any unauthorized person

B. The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability

C. Authorized access to protected information for enrollment purposes in a health insurance marketplace

D. Authorized access to information for use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability

Feedback: The correct answer is B. Information security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

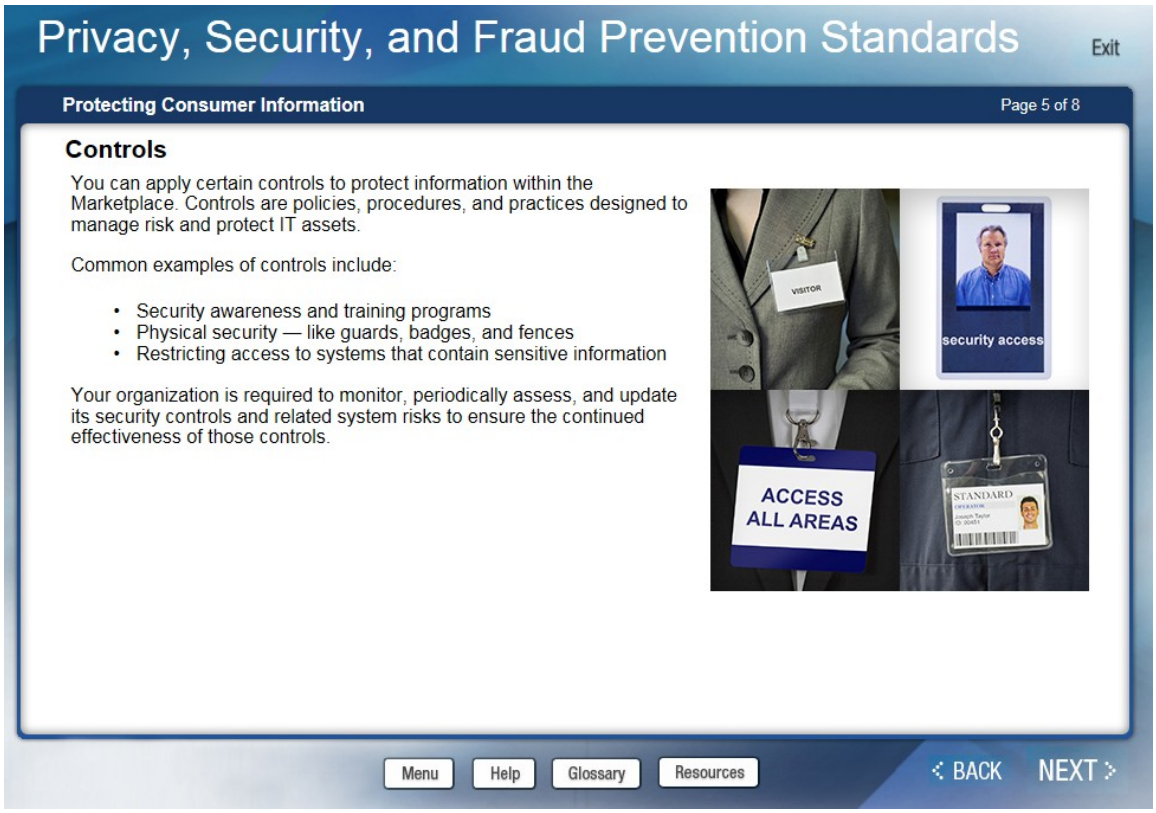
Threats to Your Computer

It's essential that any computers you use are protected from harmful computer programs, applications, and malware. It's your responsibility to ensure that any computers in your office that are used by consumers to access the Marketplace 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 cases, 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, short for malicious software, 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.

E-mail and corrupted websites may deliver malware that infect computers used to access the Marketplace. Public computers, such as those accessed in a library, may be susceptible to malware and viruses.



Controls

You can apply certain controls to protect information within the Marketplace. Controls are policies, procedures, and practices designed to manage risk and protect IT assets.

Common examples of controls include:

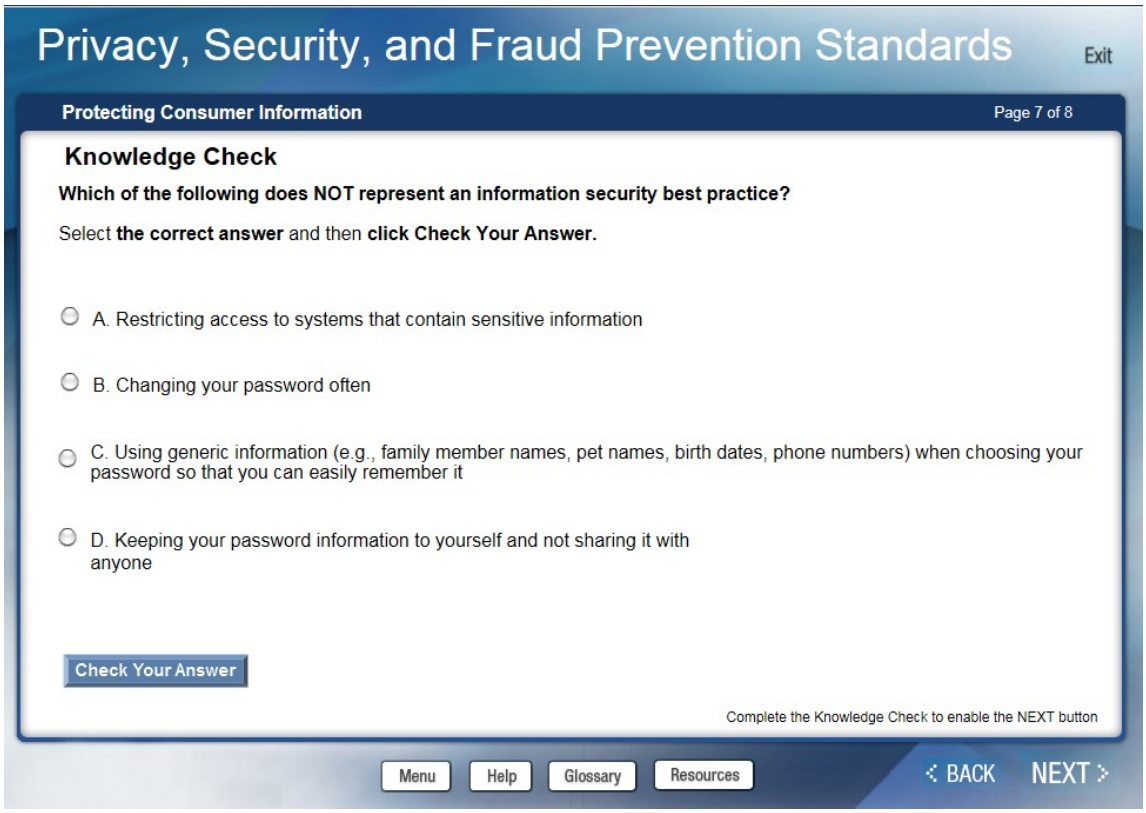
- Security awareness and training programs
- Physical security — like guards, badges, and fences
- Restricting access to systems that contain sensitive information

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

Password Protection Tips

You can take the following steps to help promote information security in the Marketplace:

- Change your password often
- Change your password immediately if you suspect it has been compromised
- Use a different password for each system or application
- When choosing your password, don't use generic information that can be easily obtained — like family member names, pet names, birth dates, phone numbers, or vehicle information
- NEVER share your password with anyone



Knowledge Check

Which of the following does NOT represent an information security best practice?

Select **the correct answer**.

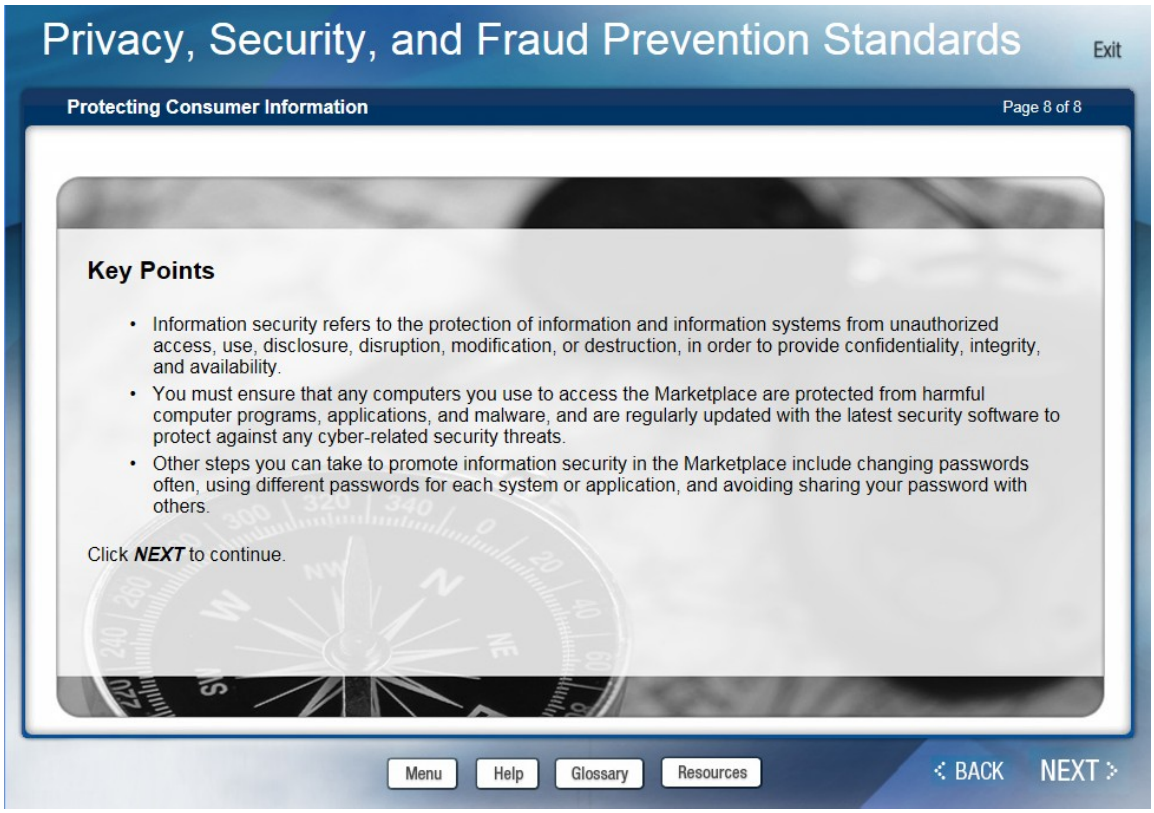
A. Restricting access to systems that contain sensitive information

B. Changing your password often

C. Using generic information (e.g., family member names, pet names, birth dates, phone numbers) when choosing your password so that you can easily remember it

D. Keeping your password information to yourself and not sharing it with anyone

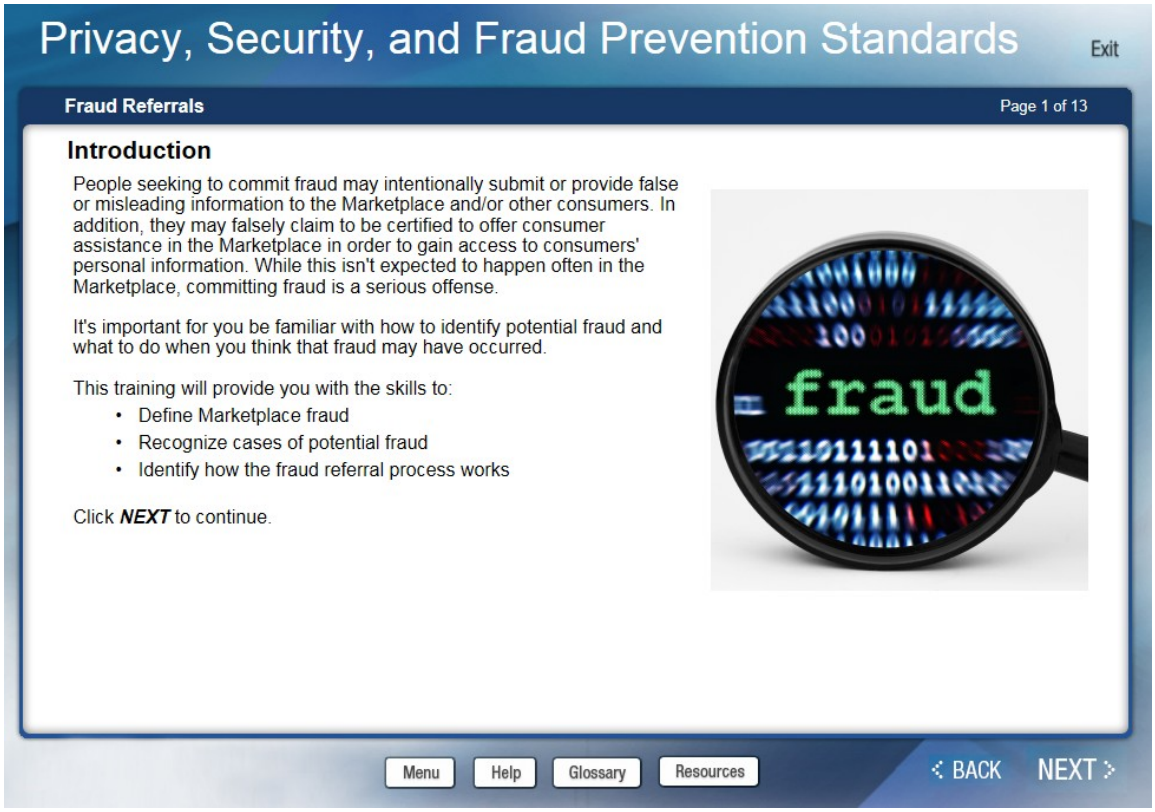
Feedback: The correct answer is C. When choosing your password, do NOT use generic information that can be easily obtained — like family member names, pet names, birth dates, phone numbers, or vehicle information.



Key Points

- Information security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, in order to provide confidentiality, integrity, and availability.
- You must ensure that any computers you use to access the Marketplace 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 steps you can take to promote information security in the Marketplace include changing passwords often, using different passwords for each system or application, and avoiding sharing your password with others.

Fraud Referrals Module



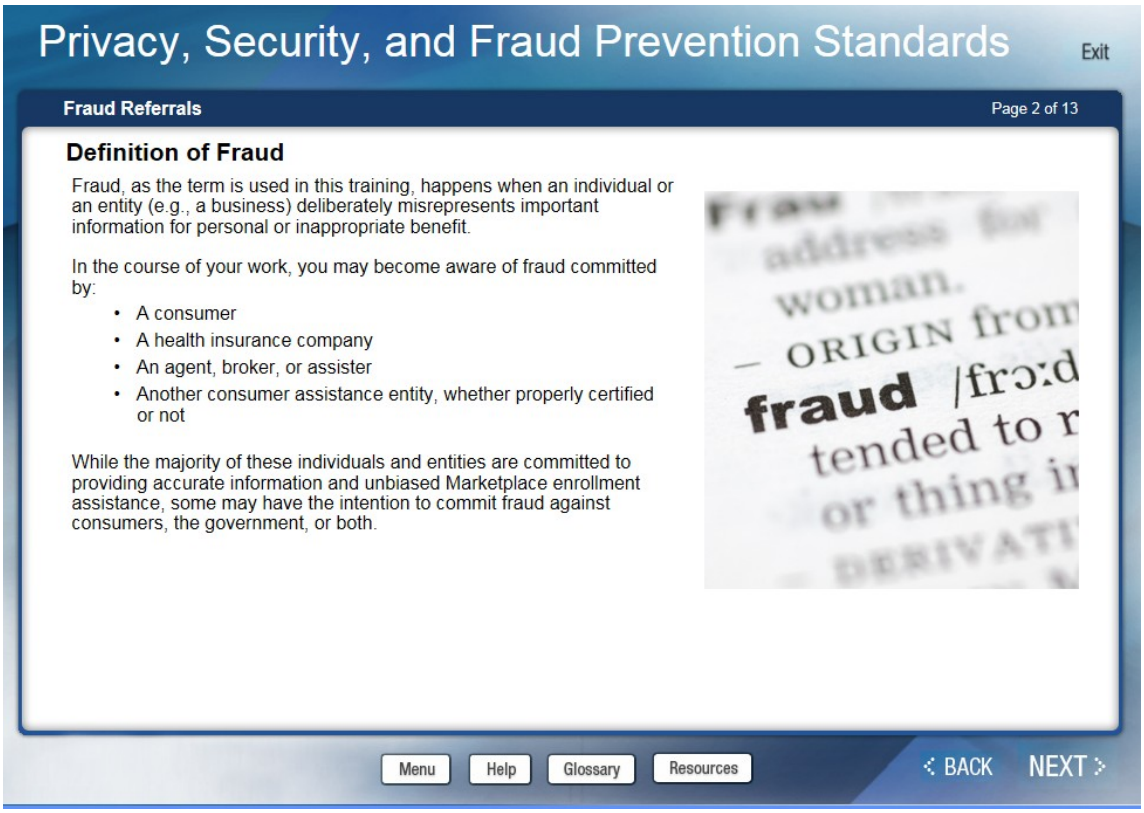
Introduction

People seeking to commit fraud may intentionally submit or provide false or misleading information to the Marketplace and/or other consumers. In addition, they may falsely claim to be certified to offer consumer assistance in the Marketplace in order to gain access to consumers' personal information. While this isn't expected to happen often in the Marketplace, committing fraud is a serious offense.

It's important for you be familiar with how to identify potential fraud and what to do when you think that fraud may have occurred.

This training will provide you with the skills to:

- Define Marketplace fraud
- Recognize cases of potential fraud
- Identify how the fraud referral process works



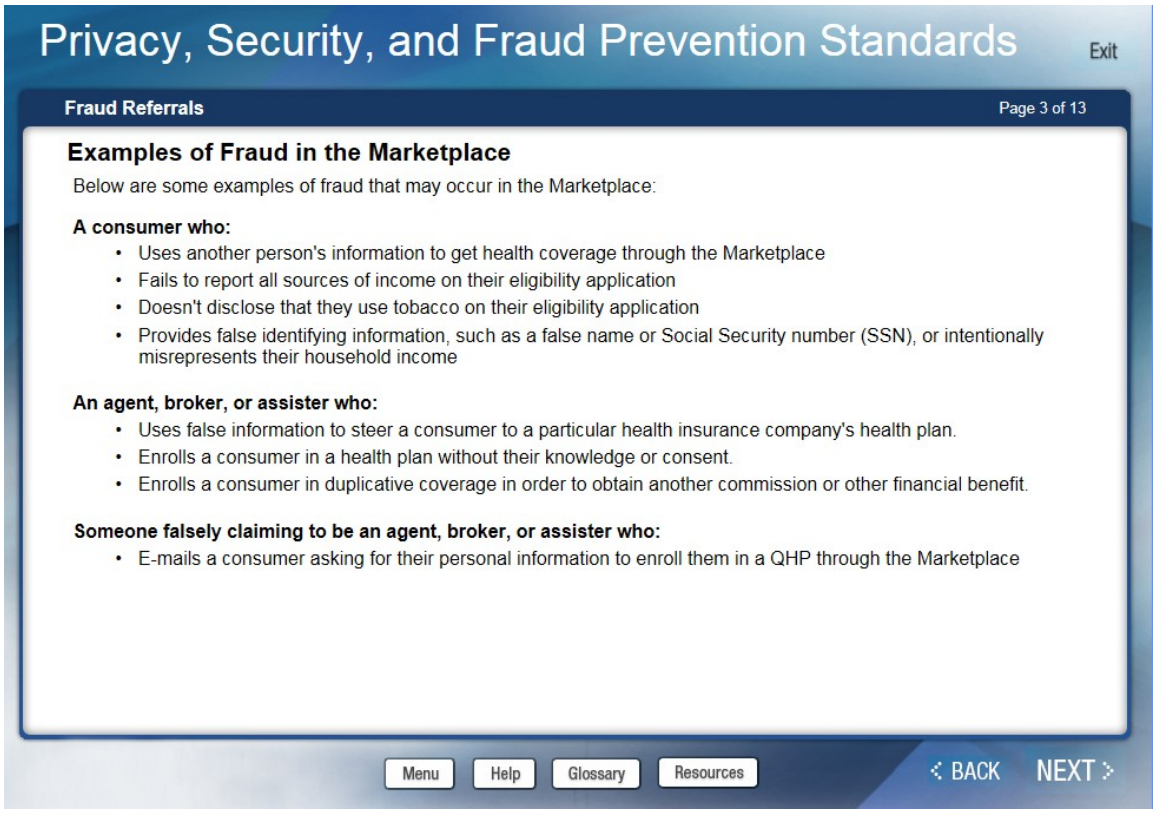
Definition of Fraud

Fraud, as the term is used in this training, happens when an individual or an entity (e.g., a business) deliberately misrepresents important information for personal or inappropriate benefit.

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

- A consumer
- A health insurance company
- An agent, broker, or assister
- Another consumer assistance entity, whether properly certified or not

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



Examples of Fraud in the Marketplace

Below are some examples of fraud that may occur in the Marketplace:

A consumer who

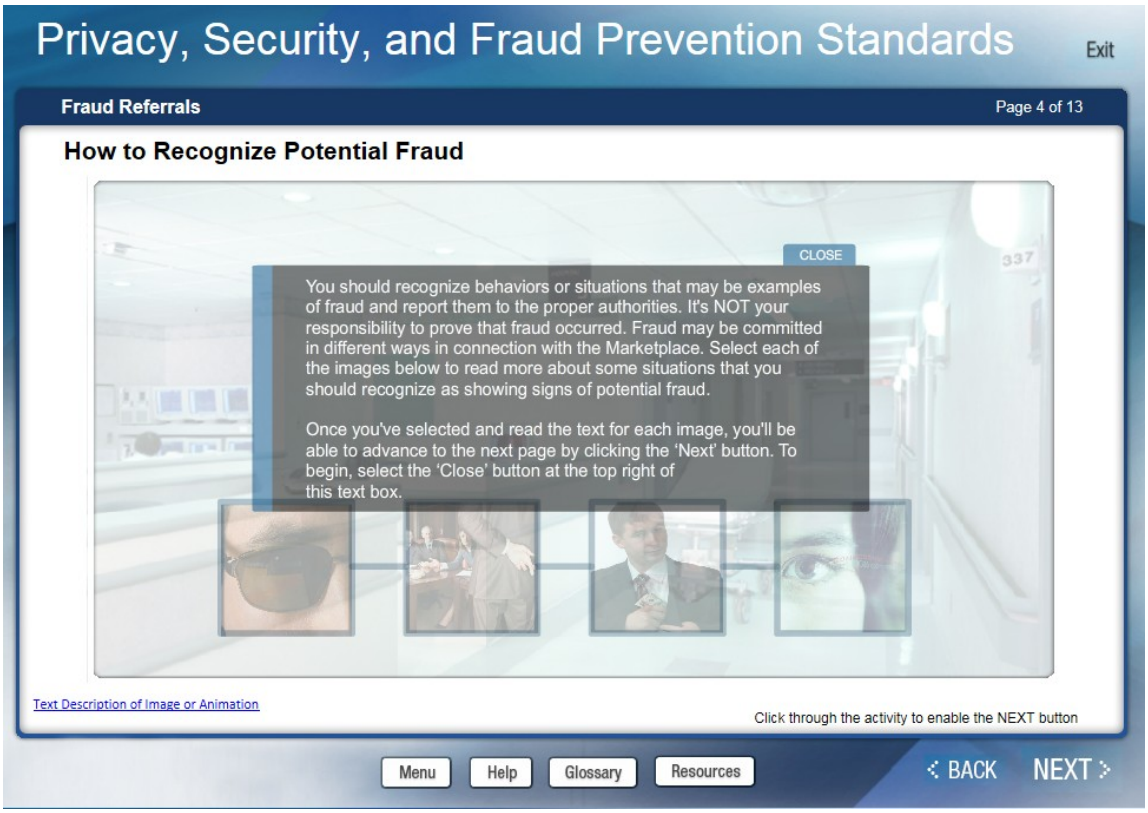
- Uses another person's information to get health coverage through the Marketplace
- Fails to report all sources of income on their eligibility application
- Doesn't disclose that they use tobacco on their eligibility application
- Provides false identifying information, such as a false name or Social Security number (SSN), or intentionally misrepresents their household income

An agent, broker, or assister who

- Uses false information to steer a consumer to a particular health insurance company's health plan.
- Enrolls a consumer in a health plan without their knowledge or consent.
- Enrolls a consumer in duplicative coverage in order to obtain another commission or other financial benefit.

Someone falsely claiming to be an agent, broker, or assister who:

- E-mails a consumer asking for their personal information to enroll them in a QHP through the Marketplace



How to Recognize Potential Fraud

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 Marketplace.

Fraud committed by a consumer

Consumers could give false information to qualify for certain types of health coverage in the Marketplace. Consumers may knowingly misrepresent facts (e.g., personal financial information or number of dependents) to get health coverage through Medicaid or the Children's Health Insurance Program (CHIP) or to get more favorable advance payments of the premium tax credit or cost-sharing reductions through the Marketplace.

Fraud or misrepresentation committed by a health insurance company

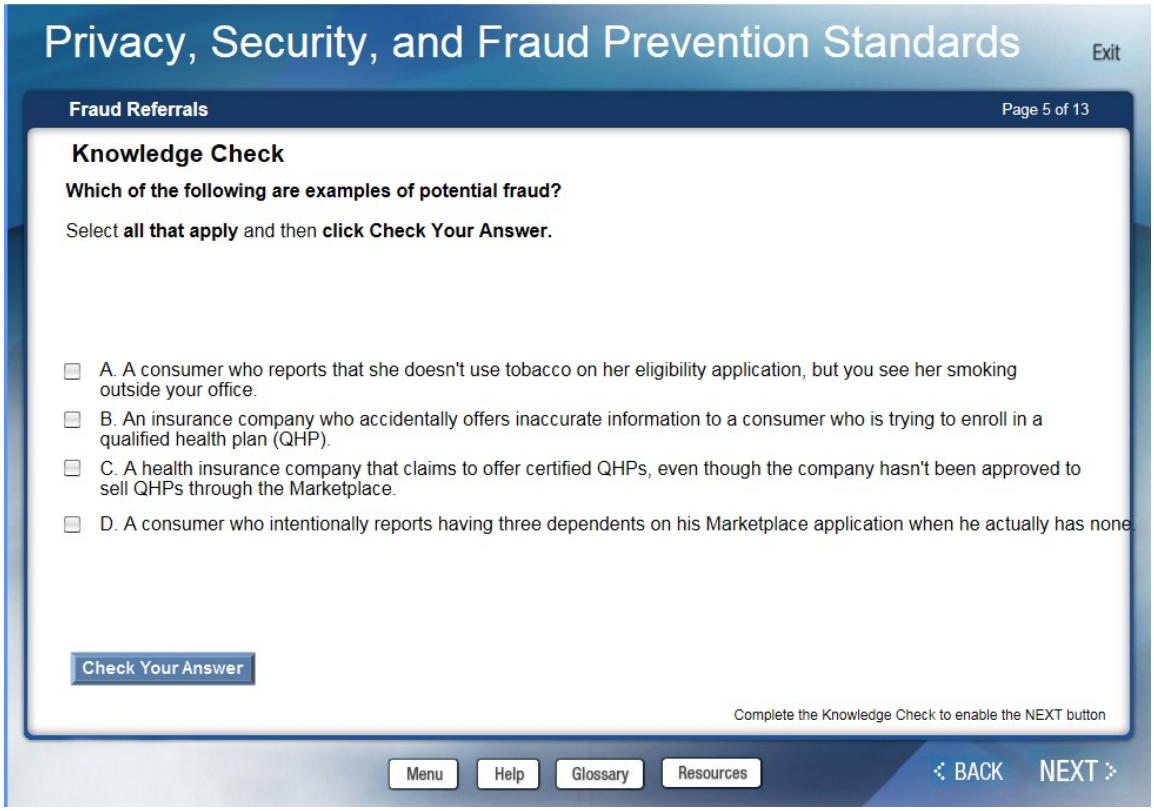
A health insurance company could give false information to attempt to convince consumers to enroll in its health plan or to not enroll consumers if insuring them could be expensive. A health insurance company might also promise consumers certain services or prices, but then not offer them the services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

Fraud committed by an agent or broker

An agent or broker may misrepresent information to convince consumers to enroll in a health plan that the agent or broker represents. The agent or broker may knowingly promise consumers certain services or prices that aren't actually available. Agents or brokers may also lie to consumers and say that they represent the Marketplace when they don't in order to get consumers' personal information or to convince consumers to enroll in non-Marketplace plans.

Fraud committed by another consumer assistance entity

Similar to a fraudulent agent or broker, another consumer assistance entity, an individual, or organization, may also lie to consumers and say that they are certified in the Marketplace when they aren't in an attempt to get consumers personal information.



Knowledge Check

Which of the following are examples of potential fraud?

Select **all that apply**.

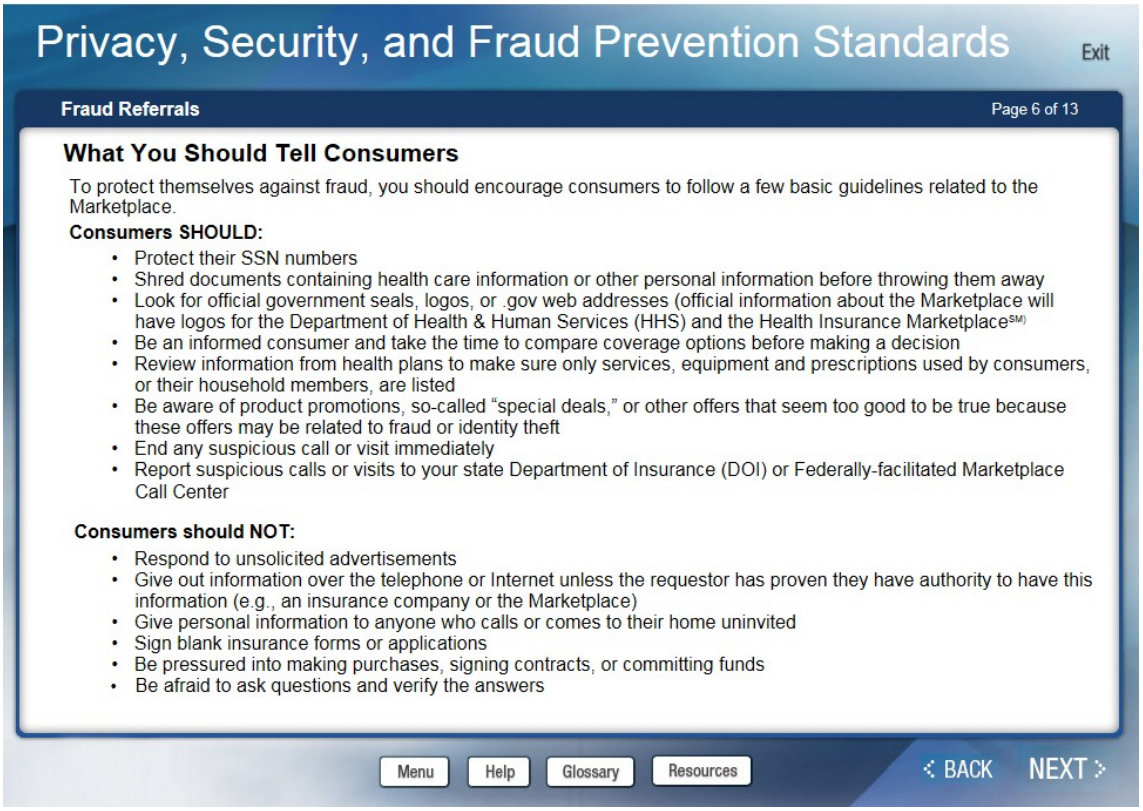
A. A consumer who reports that she doesn't use tobacco on her eligibility application, but you see her smoking outside your office.

B. An insurance company who accidentally offers inaccurate information to a consumer who is trying to enroll in a qualified health plan (QHP).

C. A health insurance company that claims to offer certified QHPs, even though the company hasn't been approved to sell QHPs through the Marketplace.

D. A consumer who intentionally reports having three dependents on his Marketplace application when he actually has none.

Feedback: The correct answers are A, C, and D. 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 Marketplace 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 Marketplace.

Consumers SHOULD

- Protect their SSN numbers
- Shred documents containing health care information or other personal information before throwing them away
- Look for official government seals, logos, or .gov web addresses (official information about the Marketplace will have logos for the Department of Health & Human Services (HHS) and the Health Insurance Marketplace℠)
- Be an informed consumer and take the time to compare coverage options before making a decision
- Review information from health plans to make sure only services, equipment and prescriptions used by consumers, or their household members, are listed
- Be aware 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 (DOI) or Federally-facilitated Marketplace Call Center

Consumers should NOT

- Respond to unsolicited advertisements
- Give out information over the telephone or Internet unless the requestor has proven they have authority to have this information (e.g., an insurance company or the Marketplace)
- Give personal information to anyone who calls or comes to their home uninvited
- 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 against fraud by:

- Protecting consumers' private health care and financial information, and reminding them to be cautious when giving out their SSN, credit card number, or banking information
- Encouraging consumers to accurately answer application questions

Consumers' SSN's, if available, should be provided only to the Marketplace and will be used for these purposes:

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

Remember, you and the Marketplace can't require any consumers who aren't seeking coverage for themselves to provide a SSN, unless information about the individual's income is necessary to determine the applicant's household income, or unless an individual's taxpayer identification number must be provided as part of a SHOP employer

application under 45 CFR §155.730. (Note: an individual is not required to provide his or her SSN if he or she is not applying for coverage for himself or herself, but if the individual's income is included in the applicant's household income, providing this information can help speed up the verification process.)

You should also reassure consumers that it's your job to provide accurate and impartial information, and to make sure that they have access to the resources they need to make informed decisions about getting health coverage through the Marketplace.

Information Needed To Report Suspected Fraud

If consumers feel that they have experienced fraud or have been the victim of identity theft, you are 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 that you or the consumer can accurately report it to the proper authorities.

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 for when the suspected fraud occurred
- Whether you suspected the fraud or heard about it from a third party (note that if the third party was a consumer, then 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 then report suspected Once you've collected the necessary information, you can then report suspected fraud. Consumers who tell you that 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 (DOI) or other state agency that regulates your activities as an assister.
- Direct consumers who believe that 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
- Consumers can also 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 number with the National Do Not Call Registry online or by phone at 1-888-382-1222

- Inform consumers that they should review their Explanation of Benefits from their insurance company for medical bills for services or equipment that they didn't receive

Role of the Office of the Inspector General

If you believe that a consumer falsified information in order to enroll in health coverage through the Marketplace, 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 health coverage, you are 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 see if fraud actually occurred. The next steps that they take can 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. One case may be closed quickly, while another case may take a long time to resolve. 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 Marketplace.

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 PO 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

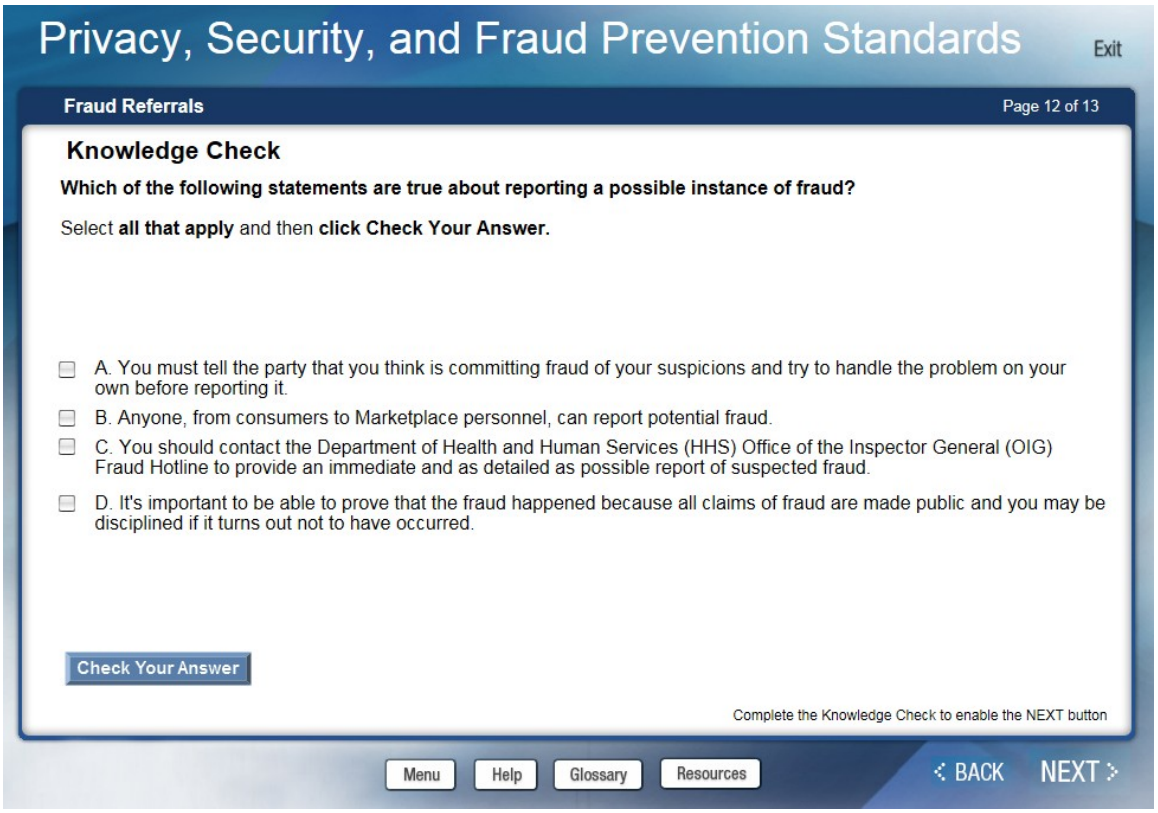
State Department of Insurance (DOI)

Contact to report agent/broker fraud. Contact your state DOI (or other state agency that regulates your activities as an assister).

Federally-facilitated Marketplace Call Center

Contact to report a complaint about an assister.

Phone: 1-800-318-2596; TTY: 1-855-889-4325 (all languages available)



Knowledge Check

Which of the following statements are true about reporting a possible instance of fraud?

Select **all that apply**.

A. You must tell the party that you think is committing fraud of your suspicions and try to handle the problem on your own before reporting it.

B. Anyone, from consumers to Marketplace personnel, can report potential fraud.

C. You should contact the Department of Health and Human Services (HHS) Office of the Inspector General (OIG) Fraud Hotline to provide an immediate and as detailed as possible report of suspected fraud.

D. It's important to be able to prove that the fraud happened because all claims of fraud are made public and you may be disciplined if it turns out not to have occurred.

Feedback: The correct answers are B and C. Fraud should always be reported immediately with as much information as possible. The HHS OIG will research each fraud referral form to see 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 consumer assistance entities.
- 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 Marketplace.
- Any incidences of suspected fraud should be reported to the HHS OIG Fraud Hotline by phone, e-mail, fax, or mail.
- All fraud reports are confidential. You or your consumers won't be penalized for submitting reports for investigation.

You've successfully completed this course.

Privacy, Security, and Fraud Prevention Resources

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

https://marketplace.cms.gov/technical-assistance-resources/assister-programs/guidance-regulations-on-assister-programs.html

CMS Risk Management Handbook Standard 7.1 Incident Handling and Breach Notification

This handbook addresses CMS' breach and incident handling procedures.

http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_7-1_Incident_Handling_Standard.pdf

National Do Not Call Registry Online

Official national do not call registry website where phone numbers can be registered and complaints can be filed.

http://www.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 U.S. Department of Health and Human Services' programs.

https://forms.oig.hhs.gov/hotlineoperations/

Secure Complaint Form

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

http://www.ftccomplaintassistant.gov/

Navigator Final Rule

This final rule addresses various requirements applicable to Navigators and non-Navigator assistance personnel in Federally-facilitated Marketplaces, and to non-Navigator assistance personnel in State-based Marketplaces that are funded through federal Exchange Establishment grants.

http://www.gpo.gov/fdsys/pkg/FR-2013-07-17/pdf/2013-17125.pdf

Certified Application Counselor Final Rule

This final rule addresses various requirements applicable to Certified Application Counselors and Certified Application Counselor Organizations.

http://www.gpo.gov/fdsys/pkg/FR-2013-07-17/pdf/2013-17125.pdf

Harmonized Security and Privacy Framework

Official CMS guidance on federal privacy and security requirements.

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