Introduction

Privacy and Security Standards

Course Introduction

Overview
This course provides training on privacy and security standards applicable under Title 45 of the Code of Federal Regulations (CFR), Section 155.260.

The course covers:

• Protecting consumer information and information security
• Restrictions on the use and disclosure of personally identifiable information (PII)
• The importance of protecting federal tax information (FTI)
• Responsibilities in maintaining confidentiality

It concludes with an exam that tests knowledge on concepts covered throughout the course.

Click NEXT to begin.
Privacy and Security Standards

Course Introduction

How to Navigate this Training

Navigation

- Use the BACK and NEXT buttons at the bottom of the page to move forward and backward in a module.
- Use the Menu button at the bottom of the page to go to any module in the course.
- Use the Resources and Glossary buttons for additional information.
- Use the Help button for a more detailed explanation of the navigation features in this course.
- Use the Exit button at the top right corner to close this course. This course contains a bookmarking feature, which lets you to exit the training at any point and return to the place you left off at a later time.

Note: If you exit during an exam, any previous answers will be lost and you’ll be required to restart the exam from the beginning during your next session. Once you have started an exam, you must complete it. If you need to stop and return to it later, your progress will not be saved. You will need to start the exam over from the beginning.

About this Course

This course doesn’t contain audio. You don’t need speakers or a headset unless you are working with assistive technology. For assistance with accessibility options, please select the Help button located at the bottom of the page.

This course contains knowledge checks or practice exercises to help prepare you for the exam you’re required to take at the end of each course.
Privacy and Security Standards

Protecting Information and Information Security

Introduction to Protecting Information and Information Security

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) and federal tax information (FTI) when you’re helping someone enroll.

This training will provide you with the skills to:

- Identify PII and FTI
- Use best practices to protect PII and FTI

Click NEXT to continue.
Privacy and Security Standards

Protecting Information and Information Security

Understanding Privacy Practices

Information privacy involves protecting an individual's personal information from unauthorized use or disclosure. Developing a set of fair information privacy practices to protect 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.

The Marketplace places a high value on privacy. It seeks to maintain consumer trust in its ability to protect a consumer's sensitive and personal information. The Marketplace has standards for privacy and security of PII and FTI.

The Marketplace privacy guidelines provide consumers with information on how their personal information is used or shared and provide protections to prevent consumers from having their personal information used or shared in a harmful way. Consumers will be informed how their PII and FTI will be used.
Privacy and Security Standards

Examples of Privacy Practices in the Marketplace

Some examples of Marketplace requirements in privacy are:

- Letting consumers know, in writing, what personal information is collected, why it's collected, how it will be used and maintained, and when the information can be shared
- Collecting only the information that's necessary to accomplish an authorized purpose
- Asking consumers to sign consent forms indicating that they understand how the Marketplace collects, uses, shares, and maintains their personal information
- Having policies and procedures for protecting and securing all personal information
- Complying with all applicable privacy and security requirements and Internal Revenue Service (IRS) rules

This information was included in the privacy and security requirements detailed in the information you or your organization received when you were approved to provide assistance to consumers. You should be familiar with these best practices to ensure that consumers' privacy is maintained.
Privacy and Security Standards

Protecting Information and Information Security

PII Definition

When interacting with consumers, you're likely to be exposed to personal information that the consumer would not want shared. PII is a type of information that can be used to distinguish or trace a consumer's identity.

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
- Biometric records (e.g., fingerprints)
- Medical, educational, financial, and/or employment information
- Phone number
- Home address
- Driver's license number
Privacy and Security Standards

Protecting Information and Information Security

Federal Tax Information (FTI) Definition

For your purposes when working in the Marketplace, FTI is defined as information disclosed by the IRS or re-disclosed by an authorized recipient who got the information from the IRS. FTI is classified as confidential and may not be used or disclosed except as expressly authorized by the IRS.

This information includes, but is not limited to:

- Electronic or paper tax returns or forms (e.g., 1040, 941, 1099, 1120, and W-2)
- Tax return information, which includes a taxpayer's name, mailing address, and identification number (e.g., SSN or Employer Identification Number [EIN])
- Information pulled from a tax return (e.g., names of dependents or the location of a business)
- Information on whether a tax return was, is being, or will be examined or subject to other investigation or processing
- Information about the consumer's income, personal finances, debts, deductions, and exemptions
- Any action taken by the IRS against the consumer (e.g., an investigation or a penalty)
- Any private written agreements between the consumer and the IRS (e.g., pricing agreements) and any background information about these agreements

Before you assist consumers, you should become familiar with what information is considered FTI and be able to recognize it when you see it.
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 you take to protect her privacy. How should you reassure her?

Select all that apply and then click Check Your Answer.

- A. Tell Sunny how you work to protect her privacy, including what information is collected, why it's collected and how it will be used and maintained, and if the information will be shared.
- B. Give Sunny a list of the information that might be collected, used, shared, and maintained.
- 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 will be sent a group of forms to sign later, but she should provide her information to you now so she can enroll for coverage through the Marketplace.
Privacy and Security Standards

Protecting Information and Information Security

Instances When You May Come in Contact with PII and FTI

As you assist consumers applying for coverage through the Marketplace, you’re likely to either collect or come in contact with PII or FTI to:

- Get a consumer’s authorization to create a Marketplace account
- Help a consumer with the eligibility process and application for health coverage
- Help a consumer assess their options for lowering costs of health coverage
- Assist a consumer with enrolling in a qualified health plan (QHP)
- Help a consumer with the application for an exemption from the individual responsibility requirement
- Assist a consumer with requesting an eligibility appeal

Remember that you should never retain consumers’ PII or FTI after their session with you has ended.
Privacy and Security Standards
Protecting Information and Information Security

Consumer Authorization Privacy Requirements
Before you begin assisting consumers, you should explain to them how their PII and FTI will be collected and used. It’s very important that you:

- Tell consumers how their PII and FTI information will be used and stored. This information was included in the privacy and security requirements detailed in the information you or your organization received when you were approved to perform these duties.
- Obtain consumer consent by using a consent form approved by the Centers for Medicare and Medicaid Services (CMS). Consent forms should be stored and protected as described in the privacy and security requirements you or your organization received when you were approved to perform these duties.

You can also tell them that PII and FTI will be used to:

- Determine eligibility for health coverage through the Marketplace
- Determine eligibility for programs to lower costs of health coverage (premium tax credits and/or cost-sharing reductions)
- Display QHP options

Explain that the Marketplace and Marketplace entities (like you and your organization) have privacy and security standards and procedures in place to protect consumers’ information. Assure consumers that PII and FTI that is collected will only be used for assisting with Marketplace functions, nothing else.
Privacy and Security Standards
Protecting Information and Information Security

Marketplace Standards for Protecting PII and FTI
You must abide by the Exchange and non-Exchange entity privacy and security standards (the Exchange is also known as the Marketplace). The standards are supported by written policies and procedures that should have been distributed to you or your organization when you were approved to provide assistance to consumers.

These policies and procedures include, but aren't limited to:

• Consumers have a right to access their records in the Marketplace.
• The Marketplace, including individuals and organizations approved to provide assistance to consumers in the Marketplace, must ensure openness and transparency about policies and procedures that directly affect consumers.
• Consumers are provided a reasonable opportunity and capability to make informed decisions about the creation, collection, disclosure access, maintenance and storage, and use of their PII.
• Information collected can only be used for Marketplace functions. It can never be used to discriminate against a consumer.
• The Marketplace and Marketplace entities approved to provide assistance to consumers in the Marketplace are responsible for data quality and integrity and must have procedures in place to assure that data is not altered or lost.
• The Marketplace and Marketplace entities approved to provide assistance to consumers in the Marketplace are accountable for appropriate monitoring and other means to identify and report incidents or breaches of security (e.g., lost records, emailing PII or FTI).
Privacy and Security Standards

Protecting Information and Information Security

Best Practices to Protect PII and FTI

Remember that you'll come in contact with PII when you assist consumers with the Marketplace eligibility and enrollment process. However, you should never enter any consumer PII or FTI or retain PII or FTI after your sessions with consumers have ended. The list below contains tips that will help you protect the information that you come into contact with.

Always
- Ensure that consumers take possession of their documents and mail their own written applications
- Secure consumer consent forms
- Verify that all scanning and copying equipment that may be used by consumers doesn't electronically retain copies of the images

Never
- Have documents containing consumer PII or FTI in your possession – always return them to the consumer at the end of each session
- Keep notes that contain a consumer's PII
- Write down a consumer's ID or password to their Marketplace account
- Enter any PII for the consumer on their application
- Send PII in an email and never solicit a consumer to send you their PII via email
- Leave a voicemail for a consumer containing any of their PII
- Leave documents with PII unattended when working with someone
- Leave PII on a computer screen which is visible to others
Remember that when you're exposed to PII or FTI, you should never retain copies or keep records of it. Always ensure that any hard copies of consumers’ records are returned prior to them departing your facility. If PII or FTI is left with you by accident, take immediate measures to have the consumer pick up the information and follow the procedures of the Marketplace and your organization for this issue.
Privacy and Security Standards

Protecting Information and Information Security

File a Breach Report

If you learn of a security issue in which a consumer’s PII or FTI has been compromised in any way, including unauthorized persons seeing or possessing the information or losing the records, the incident should be reported immediately. The Marketplace, and Marketplace entities approved to provide assistance to consumers in the Marketplace, should have written procedures in place for addressing security issues.

Issues you should report include:

- Lost, stolen, or misplaced records
- Unauthorized personnel seeing or possessing PII or FTI information
- Emailing PII or FTI between staff members
- Instances you recognize as opportunities for compromising consumer information

When a consumer’s FTI is breached, you may be required to report this to the Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards. More information on FTI security breaches can be found in IRS Document 1075.
Privacy and Security Standards

Protecting Information and Information Security

Consequences of Not Protecting PII and FTI

It's important to protect PII and FTI so consumers feel like they can trust you with their personal information, to ensure that the consumer isn't exposed to personal risk, and so you can protect yourself. If you don't protect PII and FTI or you disclose it inappropriately, you may cause harm to the consumer and/or face disciplinary action. If you don't protect a consumer's information, any of the following might occur:

- A consumer's identity may be stolen
- You may lose the consumer's trust because consumers are sensitive about sharing their personal information
- You won't be in compliance with the standards of the Marketplace and federal Privacy Act Standards
- You may be sanctioned or have to pay a fine of up to $25,000 per violation
- You or your organization may be terminated from providing Marketplace assistance to consumers
Knowledge Check

Jocelyn has been helping Julio and Anna 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 accidentally 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 all that apply and then click Check Your Answer.

- A. Jocelyn should follow the couple out with the papers, in the hope she can catch them and return the papers.
- B. Jocelyn should scan and email the documents to her boss so 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) and federal tax information (FTI).
- D. Jocelyn should put the information in her drawer, knowing they will be back in a few minutes.
Privacy and Security Standards
Protecting Information and Information Security

Key Points

While you're likely to come in contact with PII or FTI when helping a consumer in the Marketplace eligibility and enrollment process, you shouldn't retain any information after a session with a consumer has ended. If you do, you should be able to recognize and protect it appropriately.

Use best practices to protect PII and FTI.

You have successfully completed this course.

Click **EXIT** to leave the course and take the Privacy and Security Standards exam. Once you have started an exam, you must complete it. If you need to stop and return to it later, your progress will not be saved. You will need to start the exam over from the beginning.