

Welcome to the PROTECTING AND HANDLING PERSONALLY IDENTIFIABLE INFORMATION Module



Health Insurance Marketplace®



Health Insurance Marketplace®
Plan Year 2021



Text Description of Image
or Animation



Alt Text

See Long Description

Long Description

Animated introduction screen containing the following text at the top and left of the screen:

Welcome to the Protecting and Handling Personally Identifiable Information Module

Beneath this text on the left is the logo for the Department of Health & Human Services (HHS), which is made up of the profiles of people, stacked on top of each other, resulting in the profile of an eagle. The words "Department of Health & Human Services USA" form a circle that extends out and to the left from the profiles. To the right of the logo are the words "Health Insurance Marketplace®."

On the right side of the screen are three images from the module representing module-specific concepts. The health caduceus symbol is behind these images.

Disclaimer

The information in this training was current at the time it was published or uploaded onto the Web. Eligibility policies and Marketplace requirements may change so links to the source documents have been provided within the document for your reference. This training is not intended to grant rights or impose obligations. It may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage learners to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of the requirements.

This communication was printed, published, or produced and disseminated at U.S. taxpayer expense.



Page Text

The information in this training was current at the time it was published or uploaded onto the Web. Eligibility policies and Marketplace requirements may change so links to the source documents have been provided within the document for your reference. This training is not intended to grant rights or impose obligations. It may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage learners to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of the requirements.

This communication was printed, published, or produced and disseminated at U.S. taxpayer expense.

Alt Text

A page of text with horizontal lines across it; a red horizontal box containing the word “Disclaimer” within it

Module Objectives

As you learned in the Privacy Standards and Definitions module, agents and brokers who operate in the Health Insurance Marketplace® may gain access to personally identifiable information (PII).

Upon completion of this module, you should be able to:

- Identify the extent to which PII may be used and disclosed
- Understand when a civil money penalty may be imposed for improper use or disclosure of PII
- Explain how individuals may correct their PII
- Identify types of privacy incidents
- Describe the procedures required for incident handling and breach notification

*The term "Health Insurance Marketplace®" is a registered trademark of the U.S. Department of Health & Human Services. When used in this document, the term "Health Insurance Marketplace®" or "Marketplace" refers to Federally-facilitated Marketplaces (FFM), including FFM where states perform plan management functions, and also refers to State-based Marketplaces on the Federal Platform (SBM-FP).



Page Text

As you learned in the Privacy Standards and Definitions module, agents and brokers who operate in the Health Insurance Marketplace® may gain access to personally identifiable information (PII). Upon completion of this module, you should be able to:

- Identify the extent to which PII may be used and disclosed
- Understand when a civil money penalty may be imposed for improper use or disclosure of PII
- Explain how individuals may correct their PII
- Identify types of privacy incidents
- Describe the procedures required for incident handling and breach notification

*The term "Health Insurance Marketplace®" is a registered trademark of the U.S. Department of Health & Human Services. When used in this document, the term "Health Insurance Marketplace®" or "Marketplace" refers to Federally-facilitated Marketplaces (FFM), including FFM where states perform plan management functions, and also refers to State-based Marketplaces on the Federal Platform (SBM-FP).

Alt Text

A padlock displayed in front of a screen of code

Prohibited Uses and Disclosures of PII

Agents and brokers who participate in the Marketplace must comply with the specification for prohibited uses and disclosures of PII contained in Appendix A of the “Agreement Between Agent or Broker and the Centers for Medicare & Medicaid Services (CMS) for the Individual Market Federally-facilitated Exchanges and the State-based Exchanges on the Federal Platform” (Individual Marketplace Privacy and Security Agreement) or the “Agreement Between Agent or Broker and CMS for the Small Business Health Options Programs (SHOP) of the Federally-facilitated Exchanges and State-based Exchanges on the Federal Platform” (SHOP Privacy and Security Agreement).



Health Insurance Marketplace® Plan Year 2021

- Job Aids
- Help
- Glossary
- Pause
- Mute
- Transcript

< B > N

Page Text

Agents and brokers who participate in the Marketplace must comply with the specification for prohibited uses and disclosures of PII contained in Appendix A of the “Agreement Between Agent or Broker and the Centers for Medicare & Medicaid Services (CMS) for the Individual Market Federally-facilitated Exchanges and the State-based Exchanges on the Federal Platform” (Individual Marketplace Privacy and Security Agreement) or the “Agreement Between Agent or Broker and CMS for the Small Business Health Options Programs (SHOP) of the Federally-facilitated Exchanges and State-based Exchanges on the Federal Platform” (SHOP Privacy and Security Agreement).

Alt Text

Document on a desk being signed by a pen

Protecting and Handling Personally Identifiable Information

5 / 18 | Exit >

Prohibited Uses and Disclosures of PII (continued)

Select each of the three boxes for more information about prohibited uses and disclosures of PII.

Request Citizenship/Immigration Status

Discrimination

Request Social Security Number



Health Insurance Marketplace
Plan Year 2021



[Text Description of Image
or Animation](#)



Alt Text

Screen shot of "Prohibited Uses and Disclosures of PII (continued)" page

Long Description

Interactive graphic of three boxes with text stacked top to bottom inside on the left side of the screen. To the right is a filing cabinet displaying multiple numbered file folders. When each of the three boxes is selected, a pop-up box displays accompanying text.

Select each of the three boxes for more information about prohibited uses and disclosures of PII.

The text in the boxes on the left from top to bottom: [Request Citizenship/Immigration Status](#), [Discrimination](#), [Request Social Security Number](#)

The images for each popup are:

Request Citizenship/Immigration Status: a passport on top of an American flag

Discrimination: pill bottles

Request Social Security Number: a Social Security card overlapping a 1040 form



Request Citizenship/Immigration Status Pop Up text:

Agents and brokers shall not request information regarding citizenship, status as a national, or immigration status for an individual who is not seeking coverage for himself or herself on any application.

Discrimination Pop Up text:

Agents and brokers shall not use PII to discriminate, including employing marketing practices or benefit designs that will have the effect of discouraging the enrollment of individuals with significant health needs in qualified health plans (QHPs).

Request Social Security Number Pop Up text:

Agents and brokers shall not require an individual who is not seeking coverage for himself or herself to provide a Social Security number (SSN), except if an applicant's eligibility for help with paying for coverage is reliant on a tax filer's tax return and his or her SSN is relevant to verification of household income and family size.

Corrections to PII

Agents and brokers must offer individuals and entities an opportunity to request amendment, correction, substitution, or deletion of PII that is maintained and/or stored by the agent or broker if such individual or entity believes that the PII is not...

- Accurate
- Timely
- Complete
- Relevant
- Necessary

...to accomplish a Marketplace-related function.

This is true except where the information in question originated from other sources, in which case the individual or entity should contact the originating source.

Such requests must be granted or denied within no more than 10 business days of receipt and, if applicable, the PII should be corrected, amended, substituted, or deleted in accordance with applicable law.



Page Text

Agents and brokers must offer individuals and entities an opportunity to request amendment, correction, substitution, or deletion of PII that is maintained and/or stored by the agent or broker if such individual or entity believes that the PII is not...

- Accurate
- Timely
- Complete
- Relevant
- Necessary

...to accomplish a Marketplace-related function. This is true except where the information in question originated from other sources, in which case the individual or entity should contact the originating source. Such requests must be granted or denied within no more than 10 business days of receipt and, if applicable, the PII should be corrected, amended, substituted, or deleted in accordance with applicable law.

Alt Text

An image of a user updating her personal information

Accounting for Disclosures

Agents and brokers who maintain and/or store PII shall maintain an accounting of any and all disclosures, except for those disclosures made to members of the agent's or broker's workforce who have a need for the record in the performance of their duties and the disclosures that are necessary to carry out the required functions of the agent or broker.

The accounting shall:

- Contain the:
 - Date
 - Nature
 - Purpose of such disclosures
 - Name and address of the person or agency to whom the disclosure is made
- Be retained for at least 10 years after the disclosure, or the life of the record, whichever is longer
- Be available to consumers on their request per the agent's or broker's procedures for providing access to PII



Page Text

Agents and brokers who maintain and/or store PII shall maintain an accounting of any and all disclosures, except for those disclosures made to members of the agent's or broker's workforce who have a need for the record in the performance of their duties and the disclosures that are necessary to carry out the required functions of the agent or broker. The accounting shall:

- Contain the:
 - Date
 - Nature
 - Purpose of such disclosures
 - Name and address of the person or agency to whom the disclosure is made
- Be retained for at least 10 years after the disclosure, or the life of the record, whichever is longer
- Be available to consumers on their request per the agent's or broker's procedures for providing access to PII

Alt Text

A financial form with a pen and a calculator laying on it

Knowledge Check

Which of the following are prohibited according to the specifications for prohibited uses and disclosure of PII?

Select **all that apply** and then click **Check Your Answer**.

- A. Requesting information regarding the citizenship of an individual who is not seeking coverage for himself or herself on any application
- B. Requesting an SSN of an individual who is not seeking coverage for himself or herself on any application
- C. Requesting income information for an individual who is applying for the premium tax credit through the Individual Marketplace
- D. Requesting any individual's PII to discriminate or discourage the enrollment of individuals with significant health needs in QHPs

 Check Your Answer

Reset

Prompt

Select **all that apply** and then click **Check Your Answer**.

Question

Which of the following are prohibited according to the specifications for prohibited uses and disclosure of PII?

Options

- A. Requesting information regarding the citizenship of an individual who is not seeking coverage for himself or herself on any application
- B. Requesting an SSN citizenship of an individual who is not seeking coverage for himself or herself on any application
- C. Requesting income information for an individual who is applying for the premium tax credit through the Individual Marketplace
- D. Requesting any individual's PII to discriminate or discourage the enrollment of individuals with significant health needs in QHPs

Correct Answer

A, B, D



Positive Feedback

Correct! An agent or broker may not request information regarding citizenship or the SSN of an individual who is not seeking coverage for himself or herself, except that an agent or broker may request an SSN if an applicant's eligibility relies on a tax filer's tax return and his or her SSN is relevant to verification of household income and family size. Agents and brokers may not use information obtained to discriminate in marketing or benefit design. An agent or broker may collect income information from an individual to assist in obtaining a determination as to whether he or she qualifies for the premium tax credit through the Marketplace.

Negative Feedback

Incorrect. The correct answers are A, B, and D. An agent or broker may not request information regarding citizenship or the SSN of an individual who is not seeking coverage for himself or herself, except that an agent or broker may request an SSN if an applicant's eligibility relies on a tax filer's tax return and his or her SSN is relevant to verification of household income and family size. Agents and brokers may not use information obtained to discriminate in marketing or benefit design. An agent or broker may collect income information from an individual to assist in obtaining a determination as to whether he or she qualifies for the premium tax credit through the Marketplace.

Penalties for Violating FFM Privacy and Security Standards

As you learned in the Marketplace Basics module included in this curriculum, CMS oversees and monitors agents and brokers who participate in the Marketplace to ensure they comply with the FFM privacy and security standards.

The Department of Health & Human Services (HHS) has also established standards of conduct for agents and brokers who participate in the Marketplace. One of these standards is that each agent and broker must protect consumer PII in accordance with the applicable version of the Privacy and Security Agreement with CMS that the agent or broker signed.

Violation of these standards of conduct may result in one or more of the following penalties:

- Termination for cause of the agent's or broker's Agreement(s), which effectively bars the agent or broker from assisting consumers with enrollment through the Marketplace for the duration of the current plan
- Denial of the right to enter into Agreement(s) with CMS to participate in the Marketplace in future years
- Imposition of a civil money penalty of not more than \$28,906* per person or entity, per use or disclosure, against any person who knowingly and willfully uses or discloses PII in violation of section 1411(g) of the Affordable Care Act

*2019 maximum penalty amount

If HHS terminates the agent's or broker's Agreement(s), the agent or broker must continue to protect any PII accessed during the term of the Agreement(s) until such PII is appropriately destroyed or disposed of at the end of the required retention period.



Page Text

As you learned in the Marketplace Basics module included in this curriculum, CMS oversees and monitors agents and brokers who participate in the Marketplace to ensure they comply with the FFM privacy and security standards. The Department of Health & Human Services (HHS) has also established standards of conduct for agents and brokers who participate in the Marketplace. One of these standards is that each agent and broker must protect consumer PII in accordance with the applicable version of the Privacy and Security Agreement with CMS that the agent or broker signed. Violation of these standards of conduct may result in one or more of the following penalties:

- Termination for cause of the agent's or broker's Agreement(s), which effectively bars the agent or broker from assisting consumers with enrollment through the Marketplace for the duration of the current plan
- Denial of the right to enter into Agreement(s) with CMS to participate in the Marketplace in future years
- Imposition of a civil money penalty of not more than \$28,906* per person or entity, per use or disclosure, against any person who knowingly and willfully uses or discloses PII in violation of section 1411(g) of the Affordable Care Act

*2019 maximum penalty amount

If HHS terminates the agent's or broker's Agreement(s), the agent or broker must continue to protect any PII accessed during the term of the Agreement(s) until such PII is appropriately destroyed or disposed of at the end of the required retention period.



Alt Text

A person stacking jenga-type blocks on top of one another; the blocks read from top to bottom: Compliance; Rules; Standards; Policies; Regulations; Law

Definitions of Privacy and Security Incidents

Security incidents are a potential threat to the integrity of PII. A security incident means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

When the security incident involves the actual or even suspected loss of PII, that incident is considered a privacy incident. Determining the difference between a non-incident and an incident is critical.

Select the **Job Aids** button for a list of privacy incidents and scenarios.



Page Text

Security incidents are a potential threat to the integrity of PII. A security incident means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. When the security incident involves the actual or even suspected loss of PII, that incident is considered a privacy incident. Determining the difference between a non-incident and an incident is critical.

Select the **Job Aids** button for a list of privacy incidents and scenarios.

Alt Text

A partial keyboard focusing in on a red button with an illustration of a pad lock and underneath the illustration the word “Security” is displayed

Examples of Privacy and Security Incidents and Non-Incidents

Select each scenario for examples of privacy and security incidents and non-incidents.



Protecting PII



Handling Documents with PII



Talking about PII

Long Description

Interactive graphic of three images. Each image is labeled and when selected associated text appears. The images and text in the boxes from left to right.

Prompt Text: Select each scenario for examples of privacy and security incidents and non-incidents.

Image #1: a thumb drive

Label #1: [Protecting PII](#)

Protecting PII Pop Up text:

Two columns are displayed.

Column One: Incident:

Text: Loss of a hard copy document or electronic device (e.g., laptop, cell phone that can store data, disk, thumb drive, flash drive, compact disc) that contains or stores PII

Column One Image: thumb drive

Column Two: Non-Incident

Text: Sharing PII with members of your workforce who have a need for it to perform their duties

Column Two Image: A person holding a smart phone; the smart phone is displaying data being uploaded to the cloud



Image #2: A desk with various items on it including glasses, a laptop, a notebook and pen, and numerous papers with pie charts

Label #2: [Handling Documents with PII](#)

Handling Documents with PII Pop Up text:

Two columns are displayed.

Column One: Incident:

Text: Leaving documents containing PII exposed in a public area

Column One Image: A desk with various items on it including glasses, a laptop, a notebook and pen, and numerous papers with pie charts

Column Two: Non-Incident

Text: Sending documents containing PII to the consumer that the PII pertains to

Column Two Image: A person sitting at a desk typing on a laptop

Image #3: A group of agents and brokers sitting around a conference table

Label #3: [Talking about PII](#)

Talking about PII Pop Up text:

Two columns are displayed.

Column One: Incident:

Text: Posting PII, whether intentionally or unintentionally, to a public website

Column One Image: A desk with various items on it including glasses, a laptop, a notebook and pen, and numerous papers with pie charts

Column Two: Non-Incident

Text: Overhearing a colleague mention that his client is interested in enrolling in a different QHP to ensure his diabetes specialist is in the provider network

Column Two Image: A computer screen displaying code

Knowledge Check

Which of the following would NOT be considered a privacy incident?

Select the best answer and then click **Check Your Answer**.

- A. Misplacement of a mobile device that contains PII
- B. Loss of PII data through theft
- C. Overhearing a private conversation in the hallway
- D. Misrouting of an email message containing PII

 Check Your Answer

Reset

Prompt

Select the best answer and then click **Check Your Answer**.

Question

Which of the following would NOT be considered a privacy incident?

Options

- A. Misplacement of a mobile device that contains PII
- B. Loss of PII data through theft
- C. Overhearing a private conversation in the hallway
- D. Misrouting of an email message containing PII

Correct Answer

C

Positive Feedback

Correct! Overhearing a private conversation in the hallway is not considered a privacy incident.

Negative Feedback

Incorrect. The correct answer is C. Overhearing a private conversation in the hallway is not considered a privacy incident

Reporting Any Incident or Breach of PII

Select each image to learn about reporting privacy incidents or breaches.

The graphic contains four image tiles, each with a question label below it:

- Image 1:** A hand holding a white envelope with a red "CONFIDENTIAL" sticker. Label: "What is a breach?"
- Image 2:** A man in a light purple shirt sitting at a desk with a laptop, talking on a mobile phone. Label: "Who is responsible for reporting a breach?"
- Image 3:** A black gavel resting on an open book. Label: "What are CMS' Incident and Breach Notification Procedures?"
- Image 4:** Two interlocking gears, one yellow and one grey. The yellow gear has the word "partnership" written on it, and the grey gear has the word "standards" written on it. Label: "What standards are there for business partners?"

At the bottom of the graphic is a navigation bar with the following elements from left to right:

- Health Insurance Marketplace Plan Year 2021
- Job Aids (stack of papers icon)
- Help (question mark icon)
- Glossary (document icon)
- Pause (two vertical bars icon)
- Mute (speaker with X icon)
- Transcript (T icon)
- Text Description of Image or Animation (text box icon)
- Navigation arrows (left arrow with B, right arrow with N)

Long Description

Interactive graphic of 4 images. Each image is labeled and when selected associated text appears.

Image #3: A gavel on top of a book.

Label #3: What are CMS' Incident and Breach Notification Procedures?

Image #4: Two wheels with the spokes locked; the grey one is displaying the word "standards"; the yellow one is displaying the word "partnership"

Label #4: What standards are there for business partners?

Prompt Text: Select each image to learn about reporting privacy incidents or breaches.

Image #1: Confidential folder with the Confidential sticker/label

Label #1: [What is a breach?](#)

What is a breach? Pop Up text:

A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses personally identifiable information for an other than authorized purpose. The determination of whether any CMS privacy incident rises to the level of a breach is made exclusively by the CMS Breach Analysis Team (BAT). Example: An agent maintains a spreadsheet with the names and contact information of the 65 clients whom he assisted with QHP selection via the Marketplace during the last Open Enrollment period. The spreadsheet also contains the QHP selection



each client made, so the agent can account for the commissions that QHP issuers owe him. The agent stores this spreadsheet on an unencrypted laptop, which is stolen out of his car. Six weeks later, an unidentified individual contacts each client listed on the spreadsheet via phone. The individual claims that the client owes additional premiums and requests the client's credit card information. The CMS BAT determines that this incident is a breach because it has posed a significant risk of financial harm to the individuals impacted.

Image #2: Man talking on phone and looking concerned

Label #2: [Who is responsible for reporting an incident?](#)

Who is responsible for reporting an incident? Pop Up text:

Agents and brokers must designate a Privacy Official, if applicable, and/or identify other personnel authorized to access PII and responsible for reporting incidents or breaches to CMS and managing their resolution.

Example Continued: When his laptop was stolen, the agent reported the theft to his agency's Privacy Official, who was responsible for reporting the incident to CMS.

Image #3: A gavel on top of a book.

Label #3: [What are CMS' Incident and Breach Notification Procedures?](#)

What re CMS' Incident and Breach Notification Procedures? Pop Up text:

Agents and brokers must have written procedures for incident handling and breach notification. These procedures must be consistent with [CMS' Incident and Breach Notification Procedures](#), and must:

- Provide details regarding the identification, response, recovery, and follow-up of incidents and breaches, which should include information regarding the potential need for CMS to immediately suspend or revoke access to the Data Services Hub for containment purposes
- Require reporting of any incident or breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within one hour of discovery

Image #4: Two wheels with the spokes locked; the grey one is displaying the word "standards"; the yellow one is displaying the word "partnership"

Label #4: [What standards are there for business partners?](#)

What standards are there for business partners? Pop Up text: Agents and brokers operating in the Individual Marketplace or SHOP must obtain prior written consent from CMS before subcontracting or delegating any of the agent or broker services or obligations.

You are also bound to require that persons whom or businesses with which you partner or contract to perform or fulfill your authorized functions (herein, your "business partners") comply with the FFM privacy and security standards. If you have a business partner that assists in performing Marketplace functions involving PII, you must legally obligate the business partner or associate to meet or exceed the same set of standards.

Beyond the requirement to meet or exceed standards, you may also want to consider addressing topics like these within legal agreements with business partners:

- How compliance is assessed
- Validation steps for PII handoffs to ensure data quality and integrity

Knowledge Check

True or False:

Any incident involving the loss or suspected loss of PII must be reported in accordance with health insurance issuer requirements.

Select the **best answer** and then click **Check Your Answer**.

- A. True
- B. False

Check Your Answer

Reset

Prompt

Select the **best answer** and then click **Check Your Answer**.

Question

True or False: Any incident involving the loss or suspected loss of PII must be reported in accordance with health insurance issuer requirements.

Options

- A. True
- B. False

Correct Answer

B

Positive Feedback

Correct! The statement is false. The agent's or broker's designated Policy Official, if applicable, and/or other personnel authorized to access PII and responsible for reporting and managing incidents or breaches, must report any incident involving the loss or suspected loss of PII consistent with CMS' Incident and Breach Notification Procedures. Any incident involving the loss or suspected loss of PII must be reported to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within one hour of discovery.



Negative Feedback

Incorrect. The statement is false. The agent's or broker's designated Policy Official, if applicable, and/or other personnel authorized to access PII and responsible for reporting and managing incidents or breaches, must report any incident involving the loss or suspected loss of PII consistent with CMS' Incident and Breach Notification Procedures. Any incident involving the loss or suspected loss of PII must be reported to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within one hour of discovery.

Knowledge Check

Which of the following are examples of practices that an agent or broker must follow with respect to PII in the Marketplace?

Select **all that apply** and then click **Check Your Answer**.

- A. Informing consumers of the collection and use of their PII
- B. Providing consumers with the opportunity to review and correct their PII
- C. Taking appropriate steps to safeguard the confidentiality of PII
- D. Reporting privacy breaches to the CMS IT Service Desk

 Check Your Answer

Reset

Prompt

Select **all that apply** and then click **Check Your Answer**.

Question

Which of the following are examples of practices that an agent or broker must follow with respect to PII in the Marketplace?

Options

- A. Informing consumers of the collection and use of their PII
- B. Providing consumers with the opportunity to review and correct their PII
- C. Taking appropriate steps to safeguard the confidentiality of PII
- D. Reporting privacy breaches to the CMS IT Service Desk

Correct Answer

A, B, C, D

Positive Feedback

Correct! An agent or broker must follow all of these practices.

Negative Feedback

Incorrect. An agent or broker must follow all of these practices.

Agent and Broker Handling of Federal Tax Information

Federal Tax Information (FTI) is classified as confidential and may not be used or disclosed except as expressly authorized by the Internal Revenue Code, which may require signed written consent of a taxpayer in certain situations.

As an agent or broker operating in an Individual Marketplace, you are not authorized to access FTI obtained by a Marketplace from the Internal Revenue Service (IRS) verification service at any time. However, it is possible that you may encounter FTI if you are an agent or broker and also a tax return preparer or work closely (e.g., share an office) with a tax return preparer (even if for a small number of clients). In this case, you are subject to the tax return preparer disclosure rules set forth in [Internal Revenue Code § 7216](#).



Page Text

Federal Tax Information (FTI) is classified as confidential and may not be used or disclosed except as expressly authorized by the Internal Revenue Code, which may require signed written consent of a taxpayer in certain situations.

As an agent or broker operating in an Individual Marketplace, you are not authorized to access FTI obtained by a Marketplace from the Internal Revenue Service (IRS) verification service at any time. However, it is possible that you may encounter FTI if you are an agent or broker and also a tax return preparer or work closely (e.g., share an office) with a tax return preparer (even if for a small number of clients). In this case, you are subject to the tax return preparer disclosure rules set forth in [Internal Revenue Code § 7216](#).

Alt Text

A building with "Internal Revenue Service" displayed

Module Summary

Select each button and review the key points of this lesson.



The screenshot shows an interactive graphic with a blue background and a collage of icons representing healthcare and technology. Three blue rectangular buttons are arranged horizontally across the bottom of the graphic. The buttons are labeled: "Roles and Responsibilities", "Incidents and Reporting", and "Compliance and Regulations". Below the buttons is a navigation bar with icons for "Job Aids", "Help", "Glossary", "Pause", "Mute", and "Transcript". To the right of the navigation bar is a text description box labeled "Text Description of Image or Animation" and navigation arrows labeled "B" and "N".

Alt Text

Screen shot of "Module Summary" page

Long Description

Interactive graphic: A collage of icons representing module-specific concepts is displayed; three equally sized rectangular buttons are shown from left to right across the bottom of the page. Each rectangular button has a label that corresponds to a key module topic or concept: [Roles and Responsibilities](#), [Incidents and Reporting](#) and [Compliance and Regulations](#). When each button is selected a pop up box appears and displays accompanying text.

Roles and Responsibilities Pop Up text:

- An agent or broker may only use or disclose PII as needed to carry out required functions.
- Consumers must have an opportunity to request correction or deletion of their PII maintained by an agent or broker.

Incidents and Reporting Pop Up text:

- A privacy incident involves the actual or even suspected loss of PII. A privacy incident can arise from any number of causes.
- An agent or broker must report all PII incidents and breaches to the CMS IT Service Desk.



Compliance and Regulations Pop Up text:

- Violation of the FFM privacy and security standards may result in the termination of the agent's or broker's Agreement(s) with CMS, denial of the right to enter into future Agreement(s) with CMS, and/or the imposition of a civil money penalty.
- FTI is confidential and special rules apply to its access and disclosure.

Module Completion

Congratulations! You have completed the module on Protecting and Handling Personally Identifiable Information.



Page Text

Congratulations! You have completed the module on Protecting and Handling Personally Identifiable Information.

Alt Text

Person standing on a mountain peak with arms outstretched