Privacy Standards and Definitions/Protecting and Handling PII/Information Security

Privacy Standards and Definitions/Protecting and Handling PII/Information Security. 1
Disclaimer ........................................................................................................................................ 3
Introduction ..................................................................................................................................... 3
Module Objectives .............................................................................................................................. 3
Privacy vs. Security ............................................................................................................................... 3
Definition of Personally Identifiable Information ............................................................................. 4
Marketplace-specific Rules .................................................................................................................. 4
Applicability to Agents and Broker .................................................................................................... 4
Specific Privacy Standards for Agents and Brokers ......................................................................... 5
Access to PII ........................................................................................................................................ 5
Privacy Notice Statement .................................................................................................................... 6
Individual Choice: Informed Consent .................................................................................................. 6
Module Summary .................................................................................................................................. 7
Protecting and Handling PII ................................................................................................................ 8
Prohibited Uses and Disclosures of PII ............................................................................................... 8
Corrections to PII .................................................................................................................................... 8
Accounting for Disclosures ................................................................................................................ 8
Definitions of Privacy and Security Incidents .................................................................................... 9
Reporting any Incident or Breach of PII ............................................................................................. 9
Agent and Broker Handling of Federal Tax Information .................................................................. 10
Special Protections that Apply to FTI ................................................................................................. 10
Special protections apply to FTI: ......................................................................................................... 10
Module Summary .................................................................................................................................. 10
Information Security ............................................................................................................................. 11
Defining Information Security ............................................................................................................. 11
Safeguards to Prevent Unauthorized Access, Use, or Disclosure ..................................................... 11
Protecting Information ....................................................................................................................... 11
Threats, Vulnerabilities, and Risks ...................................................................................................... 12
Protection Against Viruses and Malware ................................................................. 13
Controls .................................................................................................................. 13
Password Protection Tips ....................................................................................... 13
Patching ................................................................................................................... 14
Media Protection .................................................................................................... 14
Module Summary .................................................................................................... 15
Disclaimer

The information in this training was current at the time it was published or uploaded onto the web. Eligibility policies may change frequently 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 readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

Introduction

In helping consumers obtain eligibility determinations, compare plans, and enroll in qualified health plans (QHPs) through the Federally-facilitated Marketplace (FFM), agents and brokers who are registered with the FFM may gain access to personally identifiable information (PII).

Consumers are defined to include applicants, qualified individuals, enrollees, qualified employees, qualified employers, or these individuals’ legal representatives or authorized representatives.

Obtaining PII obligates anyone with access to it to ensure that the information remains private and secure. These obligations are defined within both federal and state law.

In this module, you will learn basic information on specific privacy rules for the Federally-facilitated Marketplace and how those rules apply to agents and brokers.

Module Objectives

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

- Describe the difference between privacy, security, and confidentiality
- Define PII
- Explain the “Agreement Between Agent or Broker and the Centers for Medicare & Medicaid Services (CMS) for the Federally-facilitated Exchange Individual Market” and the “Agreement Between Agents and Brokers and the CMS for the Federally-facilitated Exchange Small Business Health Options Program (SHOP)”
- Explain how individuals may access their PII
- Describe the requirements regarding the Privacy Notice Statement
- Describe the authorized functions for which an agent or broker may create, collect, disclose, access, maintain, store and use PII in the Federally-facilitated Marketplace
- Understand the requirement to obtain a consumer's informed consent for any use or disclosure outside of the authorized functions

Privacy vs. Security

How are privacy and security defined?

Privacy is an individual’s right to control the use or disclosure of personal information. An example of this is setting the privacy settings on a Facebook account so that only certain people may view, comment, or post on your Facebook page.

Confidentiality is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Security refers to the mechanisms in place to protect the confidentiality and privacy of personal information. An example of this is the microchip embedded into a charge or debit card.
Both privacy and security are operationally achieved through a blended approach of developing and implementing effective policies and procedures and applying proper controls. Privacy and security go hand-in-hand to protect PII.

**Definition of Personally Identifiable Information**

**Marketplace Definition** - For all Marketplaces, including the Federally-facilitated Marketplace, the definition for PII is information that can be used to distinguish or trace an individual's identity, alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual. This definition may be different than definitions provided under other laws. It is important that you are familiar with this federal definition and how it applies to Marketplace information.

**Policy Definition** - Per Appendix B of the "Agreement Between Agent or Broker and the Centers for Medicare & Medicaid Services (CMS) for the Federally-facilitated Exchange Individual Market" and the "Agreement Between Agents and Brokers and the CMS for the Federally-facilitated Exchange Small Business Health Options Program (SHOP)," PII is defined to have the meaning contained in Office of Management and Budget (OMB) Memoranda M-07-16 (May 22, 2007) and means information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, or biometric records, alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Section II(b) of these Agreements specifies the types of PII that an individual may encounter in performing the role of an agent or broker in the Federally-facilitated Marketplace.

**Linkable Information** - A key component to the definition is that PII involves information that is linked or linkable to a specific individual. Therefore, if it is possible to link information to an individual, this information would be considered PII, even if it has not yet been linked to that individual.

**PII Examples** - Examples of PII include name, Social Security Number, address, email address, and date of birth.

### Marketplace-specific Rules

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual Access</td>
<td>Individuals should be provided with a simple and timely means to access and obtain their PII in a readable form and format.</td>
</tr>
<tr>
<td>Correction</td>
<td>Individuals should be provided with a timely means to dispute the accuracy or integrity of their PII and to have erroneous information corrected or to have a dispute documented if their requests are denied.</td>
</tr>
<tr>
<td>Openness and Transparency</td>
<td>There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and their PII.</td>
</tr>
<tr>
<td>Individual Choice</td>
<td>Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their PII.</td>
</tr>
<tr>
<td>Collection, Use, and Disclosure Limitations</td>
<td>PII should be created, collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.</td>
</tr>
<tr>
<td>Data Quality and Integrity</td>
<td>Persons and entities should take reasonable steps to ensure that PII is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.</td>
</tr>
<tr>
<td>Safeguards</td>
<td>PII should be protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.</td>
</tr>
<tr>
<td>Accountability</td>
<td>These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.</td>
</tr>
<tr>
<td>Other State and Federal Laws</td>
<td>An agent or broker must comply with all other applicable state and federal laws related to the privacy and confidentiality of PII. Certain functions of agents and brokers may be subject to the privacy standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It is always up to each agent or broker to understand which privacy laws and regulations his or her functions are subject to, and to fully comply with those laws.</td>
</tr>
</tbody>
</table>

**Applicability to Agents and Broker**

I'm a licensed health insurance agent, and I am completing the registration requirements to assist consumers, employers, and employees obtain health coverage in one of the Federally-facilitated Marketplace states. Before I can operate in either the Individual Marketplace or the Federally-facilitated Marketplace for the Small Business Health Options Program (FF-
SHOP), I understand I must enter into an Agreement with CMS to accept and abide by the Marketplace’s privacy and security standards, which are established by CMS.

The Agreement referred to is called the “Agreement Between Agent or Broker and the Centers for Medicare & Medicaid Services (CMS) for the Federally-facilitated Exchange Individual Market” or the “Agreement Between Agents and Brokers and the CMS for the Federally-facilitated Exchange Small Business Health Options Program (SHOP),” depending on the Market to which it applies.

By signing the applicable version of this Agreement, each agent and broker agrees to comply with the Marketplace’s privacy and security standards, established by CMS, which are defined in the Agreements’ Appendix A, titled “Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities.” The Agreement specifies the types of PII that may be collected or received, the authorized uses of such PII, and requirements for its destruction. The Agreement also outlines when and how termination of the Agreement may occur.

Section II(a) of the applicable Privacy and Security Agreement identifies the authorized functions for which an agent or broker may create, collect, disclose, access, maintain, store, and use PII in the Federally-facilitated Marketplace. The authorized functions will be described later in this module.

Specific Privacy Standards for Agents and Brokers

The privacy standards for agents and brokers are described in Appendix A of the “Agreement Between Agent or Broker and CMS for the Federally-facilitated Exchange Individual Market” and the “Agreement Between Agents and Brokers and the CMS for the Federally-facilitated Exchange SHOP”.

- Implementing policies and procedures that provide access to PII upon request (Standard 1a)
- Providing a Privacy Notice Statement (Standard 2a)
- Providing opportunity to give informed consent (Standard 3a)
- Adhering to specifications for prohibited uses and disclosures of PII (Standard 4c)
- Recognizing the right to amend, correct, substitute, or delete PII (Standard 5a)
- Accounting for disclosures (Standard 5c)
- Reporting any incident or breach of PII (Standard 6a)

Access to PII

Agents or brokers must implement policies and procedures that provide access to PII upon request.

Access rights must apply to any PII that is created, collected, disclosed, accessed, maintained, stored, and used by the agent or broker to perform any of the authorized functions outlined in the “Agreement Between Agent or Broker and CMS for the Federally-facilitated Exchange Individual Market” and the “Agreement Between Agents and Brokers and the CMS for the Federally-facilitated Exchange SHOP.”

<table>
<thead>
<tr>
<th>If the consumer or entity...</th>
<th>Then the agent or broker...</th>
<th>And...</th>
</tr>
</thead>
<tbody>
<tr>
<td>requests access to PII pertaining to the consumer and/or the person the entity represents</td>
<td>must review the request</td>
<td>grant or deny access within 30 days of receipt of the request.</td>
</tr>
<tr>
<td>has not been specific in which PII he or she would like to access</td>
<td>should send the request back to the consumer or entity</td>
<td>may offer to assist the consumer in determining his/her information needs</td>
</tr>
<tr>
<td>requests a paper or electronic copy of PII, and/or requests that it be mailed</td>
<td>may charge a fee only to recoup costs for labor for copying the PII, supplies for creating a paper copy or a copy on electronic media, and/or postage if the PII is mailed</td>
<td>may charge for any costs for preparing an explanation or summary of the PII if the recipient has requested and/or agreed to receive such summary</td>
</tr>
</tbody>
</table>
Privacy Notice Statement

Prior to collecting PII, agents and brokers must provide a Privacy Notice Statement that is prominently and conspicuously displayed on a public-facing website, if applicable, or on the electronic and/or paper form the agent or broker uses to gather and/or request the PII.

The statement must contain at a minimum the following information:

- Legal authority to collect PII
- Purpose of the information collection
- To whom PII might be disclosed, and for what purposes
- Authorized uses and disclosures of any collected information
- Whether the request to collect PII is voluntary or mandatory under the applicable law
- Effects of non-disclosure if an individual chooses not to provide the requested information

The 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 “Agreement Between Agent or Broker and CMS for the Federally-facilitated Exchange Individual Market” and the “Agreement Between Agents and Brokers and the CMS for the Federally-facilitated Exchange SHOP” Appendix A Standard 2a contains more information on the requirements for a Privacy Notice Statement.

Individual Choice: Informed Consent

Agents or brokers may create, collect, disclose, access, maintain, store, and use PII from individuals or entities only for the functions and purposes listed in the Privacy Notice Statement and any relevant agreements in effect at the time the information is collected, unless the Federally-facilitated Marketplace or the agent or broker obtains informed consent from such individuals.

Any such consent that serves as the basis of a use or disclosure must:

- Be provided in specific terms and in plain language
- Identify the entity collecting or using the PII, and/or making the disclosure
- Identify the specific collections, use(s), and disclosure(s) of specified PII with respect to a specific recipient(s)
- Provide notice of an individual’s ability to revoke the consent at any time

Consent documents must be appropriately secured and retained for 10 years. Consumers must have the opportunity to rescind consent and terminate their relationship with the agent or broker at any time.

The “Agreement Between Agent or Broker and CMS for the Federally-facilitated Exchange Individual Market” and the “Agreement Between Agents and Brokers and the CMS for the Federally-facilitated Exchange SHOP” describe authorized functions for the Individual Marketplaces* and for the FF-SHOP.*

*Individual Marketplace - Section II(a) of the Agreement Between Agent or Broker and CMS for the Federally-facilitated Exchange Individual Market identifies the following authorized functions for which an agent or broker may create, collect, disclose, access, maintain, store, and use PII in the Federally-facilitated Individual Marketplace.

1. Assisting with applications for QHP eligibility
2. Supporting QHP selection and enrollment by assisting with plan selection and plan comparisons
3. Assisting with applications for the receipt of advance payment of the premium tax credit (APTC) or cost-sharing reduction (CSR), and selecting an APTC amount
4. Facilitating the collection of standardized attestations acknowledging the receipt of the APTC or CSR determination, if applicable
5. Assisting with the application for and determination of certificates of exemption
6. Assisting with filing appeals of eligibility determinations in connection with the Federally-facilitated Marketplaces
7. Transmitting information about the consumer’s decisions regarding QHP enrollment and/or CSR and APTC information to the Federally-facilitated Marketplaces
8. Facilitating payment of the initial premium amount to the appropriate QHP
9. Facilitating an enrollee’s ability to disenroll from a QHP
10. Educating consumers, applicants, or enrollees on insurance affordability programs, and if applicable, informing such individuals of eligibility for Medicaid or the Children’s Health Insurance Program (CHIP)
11. Assisting an enrollee’s ability to report changes in eligibility status to the Federally-facilitated Marketplaces throughout the plan year, including changes that may impact eligibility (e.g., adding a dependent)
12. Correcting errors in the application for QHP enrollment
13. Informing or reminding enrollees when QHP coverage should be renewed, when enrollees may no longer be eligible to maintain their current QHP coverage because of age, or to inform enrollees of coverage QHP options at renewal
14. Providing appropriate information, materials, and programs to inform and educate consumers about the use and management of their health information and services and options offered through the selected QHP and among the available QHP options
15. Contacting consumers to assess their satisfaction or resolve complaints with services provided by the agent or broker in connection with the Federally-facilitated Marketplaces or QHPs
16. Providing assistance in communicating with QHP issuers
17. Carrying out the agent’s or broker’s legal responsibilities related to QHP issuer functions in the Federally-facilitated Marketplaces, as permitted or required by the agent’s or broker’s contractual relationships with QHP issuers
18. Other functions substantially similar to those enumerated above and such other functions that may be approved in writing by CMS

*FF – SHOP* - Section II(a) of the Agreement Between Agent or Broker and CMS for the Federally-facilitated Exchange SHOP Market identifies the following authorized functions for which an agent or broker may create, collect, disclose, access, maintain, store, and use PII in the FF-SHOP.

1. Assisting with application, eligibility, and enrollment processes for QHPs offered through the FF-SHOP
2. Supporting FF-SHOP QHP selection and enrollment by assisting with plan comparisons and plan selection
3. Facilitating employer premium contribution amount selections through the FF-SHOP
4. Facilitating payment of the initial and subsequent group premium amount for FF-SHOP coverage
5. Facilitating employee and dependent enrollment and disenrollment in QHPs offered through the FF-SHOP
6. Handling FF-SHOP coverage changes throughout the plan year that may impact eligibility, including adding a new hire, removing an employee no longer employed at a company, removing an employee no longer employed full-time, and adding a child or spouse during a special enrollment period
7. Assisting with filing appeals of FF-SHOP eligibility determinations
8. Providing customer service activities related to FF-SHOP coverage if permitted under state and federal law, including correction of errors on FF-SHOP applications and policies, handling complaints and appeals regarding FF-SHOP coverage, responding to questions about FF-SHOP insurance policies, assisting in communicating with FF-SHOP issuers, assisting with communicating with state regulatory authorities regarding FF-SHOP issues, and assistance in communicating with CMS and FF-SHOP Workforces
9. Conducting quality assurance activities, including assessment of consumer satisfaction related to the agent’s or broker’s assistance with FF-SHOP coverage
10. Providing information, materials, and programs to educate consumers about the use and maintenance of their FF-SHOP health insurance coverage and policies
11. Carrying out the agent’s or broker’s legal responsibilities related to QHP issuer functions in the Federally-facilitated Marketplaces, as permitted or required by the agent’s or broker’s contractual relationships with QHP issuers
12. Other functions substantially similar to those enumerated above and such other functions that may be approved in writing by CMS

**Module Summary**

The key points of this module are:

- PII is defined as information that can be used to distinguish or trace an individual’s identity, alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual.
- Agents and brokers operating in the Federally-facilitated Marketplace:
  - May only use or disclose PII to the extent necessary to carry out the functions authorized in their Privacy and Security Agreements with CMS.
  - Must comply with the privacy and security standards established by CMS and defined in the Agreements’ Appendix A, titled “Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities.”
- Agents or brokers must implement policies and procedures that provide individuals or entities access to PII pertaining to them and/or the person they represent upon request.
- Agents and brokers must provide a Privacy Notice Statement to any individual prior to collecting that individual’s PII.
- Consumers must provide an agent or broker their informed consent for any use or disclosure of the consumer’s PII outside of the authorized functions for PII in the Federally-facilitated Marketplace.
Protecting and Handling PII

Module Objectives
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
- Identify special provisions for handling Federal Tax Information (FTI)

Prohibited Uses and Disclosures of PII
Agents and brokers must comply with the specification for prohibited uses and disclosures of PII specified in Appendix A of the “Agreement Between Agent or Broker and CMS for the Federally-facilitated Exchange Individual Market” or the “Agreement Between Agents and Brokers and the CMS for the Federally-facilitated Exchange SHOP.”

- 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.

- The Department of Health & Human Services may impose a civil money penalty of not more than $25,000 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

- 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).

- 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 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 Federally-facilitated 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 working days of receipt, and if applicable, the PII should be corrected, amended, substituted, or deleted in accordance with applicable law.

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 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.

Definitions of Privacy and Security Incidents

Security incidents are a potential threat to the integrity of PII. A security incident occurs when there has been an attempted or successful unauthorized access, use, disclosure, modification, or destruction of data, or interference with system operations in an information system.

When the security incident involves the actual or even suspected loss of PII, that incident is considered a privacy incident. Privacy incident scenarios include the following:

- Loss of electronic devices that store PII (i.e., laptops, cell phones that can store data, disks, thumb-drives, flash drives, compact disks, etc.);
- Loss of hard copy documents containing PII;
- Sharing paper or electronic documents containing PII with individuals who are not authorized to access it;
- Accessing paper or electronic documents containing PII without authorization or for reasons not related to job performance;
- Emailing or faxing documents containing PII to inappropriate recipients, whether intentionally or unintentionally;
- Posting PII, whether intentionally or unintentionally, to a public website;
- Mailing hard copy documents containing PII to the incorrect address; and
- Leaving documents containing PII exposed in an area where individuals without approved access could read, copy, or move for future

Reporting any Incident or Breach of PII

What is a Privacy Incident?

A privacy incident is a reportable event that involves PII or Protected Health Information (PHI) where there is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to PII/PHI in usable form, whether physical or electronic.

Example: An agent maintains a spreadsheet with the names and contact information of the 65 clients that he assisted with QHP selection via the Federally-facilitated 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.

What is a Breach?

A breach is a privacy incident that poses a reasonable risk of harm to the applicable individuals. Reasonable risk of harm is the likelihood that an individual may experience a substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. 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 Continued: 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 Breach Analysis Team (BAT) determines that this incident is a breach because it has posed a significant risk of financial harm to the individuals impacted.

Who is responsible for reporting an incident?

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.
What are CMS’s Incident and Breach Notification Procedures?
Agents and brokers must have written procedures for incident handling and breach notification. These procedures must be consistent with CMS’s 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 required time frames

What Standards are there for Business Partners?
Agents and brokers operating in the Individual Marketplace or Small Business Health Options Program (FF-SHOP) Marketplace 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 Marketplace’s 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:
• Privacy and security training requirements
• How compliance is assessed
• Incident response
• Validation steps for PII handoffs to ensure data quality and integrity

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 written consent of a taxpayer in certain situations.
As an agent or broker operating in an Individual Marketplace, it is possible that you may encounter FTI when assisting with eligibility appeals. 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 a small number of clients) then you are subject to the tax return preparer disclosure rules set forth in Internal Revenue Code § 7216.

Special Protections that Apply to FTI
Special protections apply to FTI:
• By law, agents and brokers may not enter into business partner agreements that authorize access to FTI except in accordance with the Internal Revenue Code and Internal Revenue Service (IRS) approval.
• If a privacy incident involves a possible improper inspection or disclosure of FTI, the individual making the observation or receiving information should contact the office of the appropriate Special Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS.
• Remember, FTI may not be disclosed to anyone without proper authorization.

Module Summary
The key points from this module are:
• 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.
• A privacy incident occurs any time people have access or potential access to PII when they are not authorized to, or for a purpose they are not authorized to do. 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.
• Tax information is confidential and special rules apply to its access and disclosure.
Information Security

Introduction/Module Objectives
Information security is vital to the Federally-facilitated Marketplace. The goal of an information security program is to understand, manage, and reduce the risk of unauthorized access to information.
As an agent or broker, you are responsible for applying certain controls and implementing specific steps to protect information within the Federally-facilitated Marketplace.

In this module, you will learn about information security and the threats and risks associated with protecting information.

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

- Define the term “information security”
- Identify three key elements to protecting information
- Identify the differences between threats, vulnerabilities, and risks to information
- Identify certain controls that agents and brokers can take to protect information within the Federally-facilitated Marketplace
- List steps that agents and brokers can take to help promote information security in the Federally-facilitated Marketplace

Defining Information Security
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 the Department of Health & Human Services (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.

Safeguards to Prevent Unauthorized Access, Use, or Disclosure
All guidance for operational, technical, administrative, and physical safeguards is found within a suite of documents called the Minimum Acceptable Risk Standards for Exchanges (MARS-E).
(Remember, Marketplaces are typically referred to as Exchanges in the Affordable Care Act and associated regulations.)


Protecting Information
Your bank ATM is a good example of an information system that must be confidential, available, and have integrity.

There are three key elements to protecting information.

- **Confidentiality:** Protecting information from unauthorized disclosure to people or processes
- **Availability:** Defending information systems and resources from malicious, unauthorized users to ensure accessibility by authorized users
- **Integrity:** Assuring the reliability and accuracy of information and information technology (IT) resources.
Imagine if your account was not kept confidential and someone else was able to access it when they approached the ATM. How much damage could be done?

Imagine if your bank was rarely available when you needed it. Would you continue to use that bank?

Imagine if every time you went to the ATM, the balance it displayed was inaccurate. How could the poor integrity of your balance information adversely affect your account management? Select the “Cancel” button to read through this information again.

**Threats, Vulnerabilities, and Risks**

Threats and vulnerabilities put information assets at risk. A threat is the potential to cause unauthorized disclosure, changes, or destruction to an asset. Impacts of a threat can include a potential breach in confidentiality, a potential breach in integrity, and the unavailability of information. There are different types of threats. Threats can be natural, environmental, and man-made.

A vulnerability is any flaw or weakness that can be exploited and could result in a breach or a violation of a system’s security policy.

A risk is the likelihood that a threat will exploit a vulnerability. For example, a system may not have a backup power source; so it is vulnerable to a threat such as a thunderstorm. The thunderstorm creates a risk to the system.

It is essential that computers used to conduct business in the Federally-facilitated Marketplace are protected from harmful computer programs, applications, and malware. As an agent or broker, it is your responsibility to ensure that the computer you use to access a Federally-facilitated Marketplace is regularly updated with the latest security software to protect against any cyber-related security threats.

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

Email and corrupted websites are among the ways that malware can infect computers used to access the Health Insurance Marketplaces. Select each image on the computer screen to learn about the various types of malware.

<table>
<thead>
<tr>
<th>Label</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td>A computer virus is a small program written to alter the way a computer operates, without the permission or knowledge of the user. With an ability to replicate itself, a virus can continue to spread and cause damage to a computer. Computer viruses can damage or corrupt data, modify existing data, or degrade the performance of the system by utilizing resources such as memory or disk space. Viruses can spread over a network or the Internet, or be carried on a removable medium such as a CD/DVD drive or Universal Serial Bus (USB) drive.</td>
</tr>
<tr>
<td>Trojan Horse</td>
<td>A Trojan horse, or Trojan, is a type of malware which gains privileged access to an operating system by appearing to perform a desirable function. Trojan horses contain malicious code that when triggered cause loss, or even theft, of data. Unlike viruses, Trojan horse programs do not replicate themselves. An example of a Trojan horse is the Trojan.Vundo program. This malware retrieves a user's name and password. It also erases or overwrites data on a computer and can spy on a user to gather his or her information such as browsing habits or sites visited.</td>
</tr>
<tr>
<td>Worms</td>
<td>Worms are programs that replicate themselves from system to system without the use of a host file. Worms are spread through local area networks, wide area networks, or through the Internet via emails, messaging, and chat functions. Worms almost always cause harm to the network, such as by consuming network bandwidth.</td>
</tr>
<tr>
<td>Spyware</td>
<td>Spyware is a type of malware that can be installed on computers, collecting small pieces of information about a user without their knowledge. The presence of spyware is typically hidden from the user (having been secretly installed), and can be difficult to detect.</td>
</tr>
</tbody>
</table>
| Adware       | Adware is any software package which automatically plays, displays, or downloads advertisements to a computer. Adware may also steal information. 
An example of adware is "Bonzi Buddy," which is marketed as an "Intelligent Software Agent." When installed, it successfully corrupts many of the user's system files. |
|-------------|---------------------------------------------------------------------------------------------------------------|
| Rootkits    | A rootkit is a piece of software that can be installed and hidden on a computer without the user’s knowledge. It may be included in a larger software package or installed by an attacker who has taken advantage of a vulnerability on the host computer or convinced the user to download it. 
Rootkits are not necessarily malicious, but they may hide malicious activities. Attackers may be able to access information, monitor the user’s actions, modify programs, or perform other functions on the host computer without being detected. 
Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it. |
| Crimeware   | Crimeware is software that performs illegal actions unanticipated by a user running the software, which are intended to yield financial benefits to the distributer of the software. |
| Scareware   | Scareware is malware that is written to look and act like a legitimate security anti-virus package in order to trick victims into buying worthless software to fix nonexistent virus or spyware problems. |

**Protection Against Viruses and Malware**

To best protect your computer, ensure that your system has up-to-date malware protections installed.

**Anti-virus software**

Anti-virus software is a computer program that identifies and removes computer viruses and other malicious software like worms and Trojan horses from an infected computer. It also protects the computer from further virus attacks.

Anti-virus software examines every file in a computer with the virus definitions stored in its *virus dictionary*: an inbuilt file that contains code identified as a virus by the anti-virus authors.

You should regularly run an anti-virus program to scan and remove any possible virus attacks from a computer. Most commercially-available anti-virus software automatically provides virus updates daily.

**Anti-spyware**

Anti-spyware can also provide real-time protection against the installation of spyware on your computer. This type of spyware protection works like anti-virus protection by scanning and blocking all incoming network threats. It also detects and removes spyware that has already been installed into the computer. Anti-spyware scans the contents of the windows registry, operating system files, and installed programs on the computer and provides a list of any threats found.

**Controls**

Agents and brokers can apply certain controls to protect information within the Federally-facilitated 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

For more information on internal controls, refer to the [MARS-E suite of documents](#).

**Password Protection Tips**

There are steps agents and brokers can take to help promote information security in the Federally-facilitated 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.
- Do not reuse a password until six other passwords have been used.
- 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.
- NEVER share your password with anyone!

**Patching**
Patches are updates issued by the vendor that fix a particular problem or vulnerability within a software program. Patch management is a critical business function for effective data risk management.

To mitigate the impact of any potential attacks, agents and brokers should ensure the operating systems and applications on their computers remain patched with the latest security updates from their vendors.

In addition to the security consequences of not installing the most recent patches to your system, recovery from attacks and infections can be expensive and prolonged. To limit risk and vulnerability, pay attention to security alerts and conduct patch management systematically. Schedule patching activities as a regular part of your business routine, and allow flexibility for emergencies.

**Media Protection**
In addition to protecting your computer and related systems, it is critical that you protect various media forms as well. Select the highlighted elements in the image to learn more.

**Protect Sensitive Unclassified Information** - Disclosure and modification of data that is not specifically authorized is prohibited. Data including consumer personally identifiable information (PII) should not be used for unauthorized or illegal purposes, for private gain, or to misrepresent oneself, or the federal government. Be mindful that copyright laws must not be violated when distributing or receiving information via public access systems.

**Protect Your Equipment** - Mobile computing devices (e.g., laptops, portable storage, memory sticks) should be secured by way of appropriate locks or other safeguards to protect from theft. Practice good housekeeping at all times, including no smoking, drinking, or eating around your personal computer or workstation. Keep electrical appliances and magnets away from your computer and storage media. Always discard consumer PII through shredding or secured refuse removal.

**Protect Your Area** - Politely challenge, and assist people who do not belong in the work area to avoid potential security attacks, such as "shoulder surfing" or "social engineering." Physical access to secured areas (e.g., data centers, wiring closets) must be limited to authorized personnel via appropriate authorization credentials (e.g., identification badges, proximity cards, smart cards).
- Physical access must be restricted from visitors before authorizing access to areas where there are information systems that contain consumer PII.
- Visitor access records for areas where there are information systems with consumer PII should be maintained and reviewed on a monthly basis.
- Arrange Workstations so that the computer screen is not visible to individuals standing at a door or when first entering the room (e.g., "shoulder surfing"). Utilize privacy filter screens as necessary.

**Printing, Faxing, and Postal Mailing** - Ensure that you safeguard printed information. Only print what is necessary, double-check the fax number before sending, and verify mailing addresses are still current. Print materials should be locked away when not in use or shredded if no longer needed. When faxing PII, ensure that the fax that the document is being sent to is not in a public area and that the individual receiving the fax is aware of this.

**Protect Email and Conversations** - Communications are encrypted when exchanging PII or other sensitive data electronically. Do not have conversations with or about people in a public area without ensuring the conversation is private. Do not conduct business on buses, trains, or mass transit.
Module Summary
The key points from this module on information security are:

- Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
- The goal of an information security program is to understand, manage, and reduce the risk to information.
- There are three key elements to protecting information: confidentiality, availability, and integrity.
- A threat is the potential to cause unauthorized disclosure, changes, or destruction to an asset. Threats can be natural, environmental, and man-made.
- A vulnerability is any flaw or weakness that can be exploited, and could result in a breach or a violation of a system’s security policy.
- A risk is the likelihood that a threat will exploit a vulnerability.
- Agents and brokers can apply certain controls – policies, procedures, and practices that manage risk and protect IT assets – to protect information within the Marketplaces.
- There are steps agents and brokers can take to help promote information security in the Marketplaces. Most importantly, NEVER share your password.