Contents

Privacy and Security Standards............................................................................................................... 3

Introduction ........................................................................................................................................ 3
Course Objectives ............................................................................................................................ 3
Privacy vs. Security .............................................................................................................................. 4
Definition of Personally Identifiable Information.................................................................................. 4
Agent and Broker Handling of Federal Tax Information......................................................................... 4
Marketplace-specific Rules ..................................................................................................................... 5
Applicability to Agents and Brokers...................................................................................................... 6
Specific Privacy Standards for Agents and Brokers ............................................................................... 6
Access to PII ....................................................................................................................................... 7
Privacy Notice Statement ...................................................................................................................... 7
Individual Choice: Informed Consent ................................................................................................... 8
Prohibited Uses and Disclosures of PII .................................................................................................. 8
Corrections to PII ................................................................................................................................. 9
Accounting for Disclosures .................................................................................................................. 9
Definitions of Privacy and Security Incidents ....................................................................................... 9
Reporting any Incident or Breach of PII ............................................................................................... 10
Retention of PII ................................................................................................................................... 10
Civil Money Penalty for Knowing and Willful Use or Disclosure of PII .................................................... 10
Obligating Business Partners to Follow the Same, or More Stringent, Standards ............................... 11
Other State and Federal Laws ................................................................................................................ 11
Topic Summary .................................................................................................................................. 11
Introduction ....................................................................................................................................... 12
Information Security Overview ............................................................................................................ 13
Safeguards to Prevent Unauthorized Access, Use, or Disclosure ........................................................ 13
Protecting Information ....................................................................................................................... 13
Threats, Vulnerabilities, and Risks ...................................................................................................... 14
Threats to Your Computer .................................................................................................................... 14
Protection Against Viruses and Malware .............................................................................................. 15
Controls ............................................................................................................................................ 15
Password Protection Tips .................................................................................................................... 15
Privacy and Security Standards

Patching............................................................................................................................................ 16
Media Protection............................................................................................................................ 16
Topic Summary............................................................................................................................... 16
Privacy and Security Standards

Introduction

In helping consumers obtain eligibility determinations, compare plans, and enroll in qualified health plans (QHPs) through the Federally-facilitated Marketplaces, agents and brokers 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 topic, you will learn basic information on specific privacy rules for the Federally-facilitated Marketplaces and how those rules apply to agents and brokers.

Course Objectives

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

- Describe the difference between privacy, security and confidentiality
- Define PII
- Identify special provisions for handling Federal Tax Information (FTI)
- 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
- Identify the extent to which PII may be used and disclosed
- Explain how individuals may correct their PII
- Identify types of privacy incidents
- Describe the procedures required for incident handling and breach notification
- Explain record retention policies
- Understand when a civil money penalty may be imposed
- Explain requirements for business partners
- Describe the relationship between state and federal laws
Privacy vs. Security

How are privacy and security defined?

Privacy is an individual’s right to control the use or disclosure of personal information.

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.

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

For all Marketplaces, including the Federally-facilitated Marketplaces, 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. Examples of PII include name, Social Security Number, address, e-mail address, and date of birth.

Two key points to remember about this definition:

1. 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.
2. 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.

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 apply to FTI:
Privacy and Security Standards

- 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.

Marketplace-specific Rules

A Marketplace needs to create and collect PII to determine eligibility for enrollment in a QHP, insurance affordability programs, and for certifications of exemption from the individual responsibility requirement to have minimum essential coverage.

Per the Affordable Care Act and 45 CFR §155.260(a)(3), a Marketplace and entities that gain access to Marketplace PII, including agents and brokers, must also establish and comply with privacy and security standards that are consistent with these eight principles:

(i) Individual Access - Individuals should be provided with a simple and timely means to access and obtain their PII in a readable form and format.

(ii) Correction - 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.

(iii) Openness and Transparency - There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their PII.

(iv) Individual Choice - Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their PII.

(v) Collection, Use, and Disclosure Limitations - 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.

(vi) Data Quality and Integrity - 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.

(vii) Safeguards - 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.
Privacy and Security Standards

(viii) **Accountability** - 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.

**Applicability to Agents and Brokers**

Agents and brokers operating in the Individual Marketplaces or the Federally-facilitated Marketplaces for the Small Business Health Options Program (FF-SHOP) (or both) must enter into an Agreement that 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. This Agreement 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. Agents and brokers may only use or disclose PII to the extent necessary to carry out the **functions authorized in these Privacy and Security Agreements**.

By signing the applicable version of this Agreement, each agent and broker consents 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.”

**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” and include:

- 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)

Additional guidance on the privacy and security standards and their implementation specifications is contained in 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” you must accept before assisting consumers with application and enrollment in a Federally-facilitated Marketplace. Next, we will walk through these seven key standards.
Access to PII

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.

- 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.”
- At the time the request is made, the individual or entity should generally be required to specify which PII he or she would like to access.
- The agent or broker 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, postage if the PII is mailed, or any costs for preparing an explanation or summary of the PII if the recipient has requested and/or agreed to receive such summary.
- The agent or broker must complete the review of a request for access or notification (and grant or deny said notification and/or access) within 30 days of receipt of the notification and/or access request.

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

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.
- 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.
- 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 QHPs.
Corrections to PII

Agents and brokers must offer individuals and entities an opportunity to request amendment, correction, substitution, or deletion of PII maintained and/or stored by the agent or broker if such individual or entity believes that the PII is not accurate, timely, complete, relevant, or necessary to accomplish a Federally-facilitated Marketplace-related function, 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

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, agents and brokers who maintain and/or store PII shall maintain an accounting of any and all disclosures.

- The accounting shall contain the date, nature, and purpose of such disclosures, and the name and address of the person or agency to whom the disclosure is made.
- The accounting shall be retained for at least 10 years after the disclosure, or the life of the record, whichever is longer.
- This accounting shall 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;
- E-mailing or faxing documents containing PII to inappropriate recipients, whether intentionally or unintentionally;
- Posting PII, whether intentionally or unintentionally, to a public website;
- Mailing hard copy documents containing PII to the incorrect address; and
• Leaving documents containing PII exposed in an area where individuals without approved access could read, copy, or move for future use.

Reporting any Incident or Breach of PII

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. Agents and brokers must report any incident involving the loss or suspected loss of PII or PHI consistent with CMS’ Incident and Breach Notification Procedures, described below.

A breach is a privacy incident that poses a reasonable risk of harm to the applicable individuals. 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).

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:

• Identify the agent’s or broker’s Designated Privacy Official, if applicable, and/or identify other personnel authorized to access PII and responsible for reporting and managing incidents or breaches to CMS
• 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

Retention of PII

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” specifies record retention periods in two instances:

• Informed Consent – Consent documents must be appropriately secured and retained for 10 years
• Accounting for PII Disclosure – The accounting for PII disclosure shall be retained for at least 10 years after the disclosure, or the life of the record, whichever is longer

Civil Money Penalty for Knowing and Willful Use or Disclosure of PII

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.
Obligating Business Partners to Follow the Same, or More Stringent, Standards

Standard 5b of Appendix A to 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” instructs agents and brokers operating in the Individual Marketplaces or FF-SHOP Marketplaces to obtain prior written consent from CMS before subcontracting or delegating any of the agent or broker services or obligations.

If you assign, subcontract, or otherwise delegate your obligations in violation of this provision, you remain legally bound and responsible for all obligations under the Agreement and are subject to compliance actions.

Your business partners are also obligated to 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

Other State and Federal Laws

An agent or broker must comply with all other applicable state and federal law 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.

Topic Summary

The key points from this topic on the privacy standards and implementation specifications are:

- In helping consumers obtain eligibility determinations, compare plans, and enroll in QHPs through the Federally-facilitated Marketplaces, agents and brokers may gain access to PII.
- 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.
Privacy and Security Standards

• Entities that gain access to Marketplace PII, including agents and brokers, must establish and comply with privacy and security standards that are consistent with eight principles described in the Affordable Care Act and 45 CFR §155.260(a)(3).
• An agent or broker may only use or disclose PII as needed to carry out required functions.
• Before assisting consumers in a Federally-facilitated Individual Marketplace or FF-SHOP, each agent and broker must accept either 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” (or both if participating in both Markets), which includes privacy and security standards for use and disclosure of PII.
• Tax information is confidential and special rules apply to its access and disclosure.
• 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.

Information Security

Introduction

Information security is vital to the Marketplaces. 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 Marketplaces.

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

Objectives

Upon completion of this topic, 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 Marketplaces
• List steps that agents and brokers can take to help promote information security in the Marketplaces
Information Security Overview

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

- Information security is achieved through implementing technical, management, and operational measures designed to protect the confidentiality, integrity, and availability of information.
- The goal of an information security program is to understand, manage, and reduce the risk to information under the control of the organization.
- In today’s work environment, many information systems are electronic; however 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

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
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.

Threats to Your Computer

It is essential that computers used to conduct business in the Federally-facilitated Marketplaces 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.

E-mail and corrupted websites are among the ways that malware can infect computers used to access the Health Insurance Marketplaces.

Types of malware include:

- Virus
- Trojan Horse
- Worms
- Spyware
- Adware
- Rootkits
- Crimeware
- Scareware
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 Marketplaces. 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 Marketplaces.

- 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 each of the following to read more:

- Protect Sensitive Unclassified Information
- Protect Your Equipment
- Protect Your Area
- Printing, Faxing, and Postal Mailing
- Protect E-mail and Conversations

Topic Summary

The key points from this topic 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.
Privacy and Security Standards

- There are steps agents and brokers can take to help promote information security in the Marketplaces. Most importantly, NEVER share your password.