Page: 1 of 24: Welcome to the INFORMATION SECURITY Module

Welcome to the
INFORMATION SECURITY
Module

Exit >
Health Insurance Marketplace®
Health Insurance Marketplace®
Plan Year 2021
Job Aids
Help
Glossary
Pause
Mute
Transcript
Text Description of Image or Animation
N

Alt Text

Welcome to the Information Security 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®.” When used in this document, the term “Health Insurance Marketplace®” or “Marketplace” refers to Federally-facilitated Marketplaces (FFMs), including FFMs where states perform plan management functions, and also refers to State-based Marketplaces on the Federal Platform (SBM-FPs). On the right side of the screen are three images from the module representing module-specific concepts.

Long Description

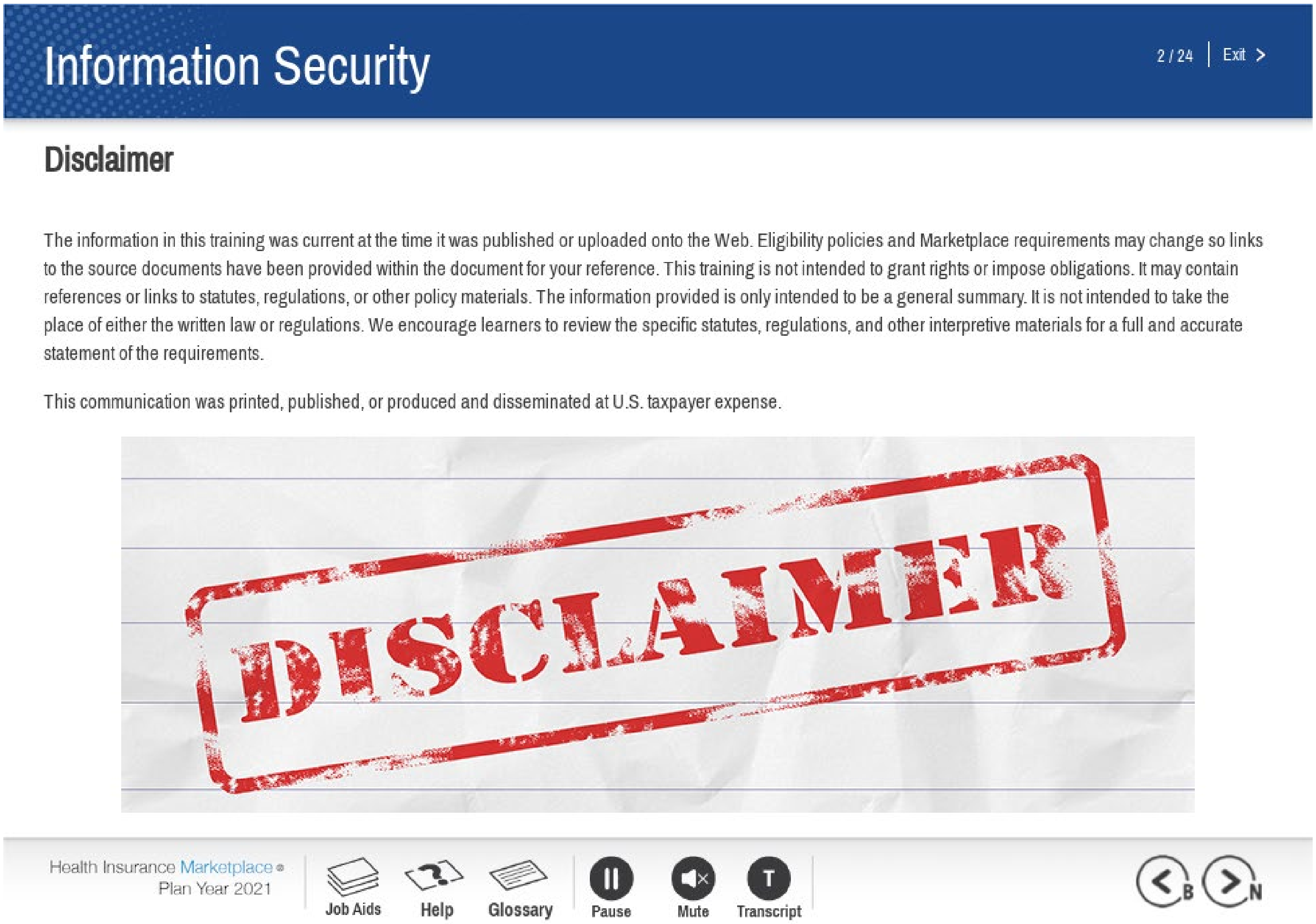
Animated introduction screen containing the following text at the top and left of the screen:

Welcome to the Information Security 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.

Page: 2 of 24: Disclaimer



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

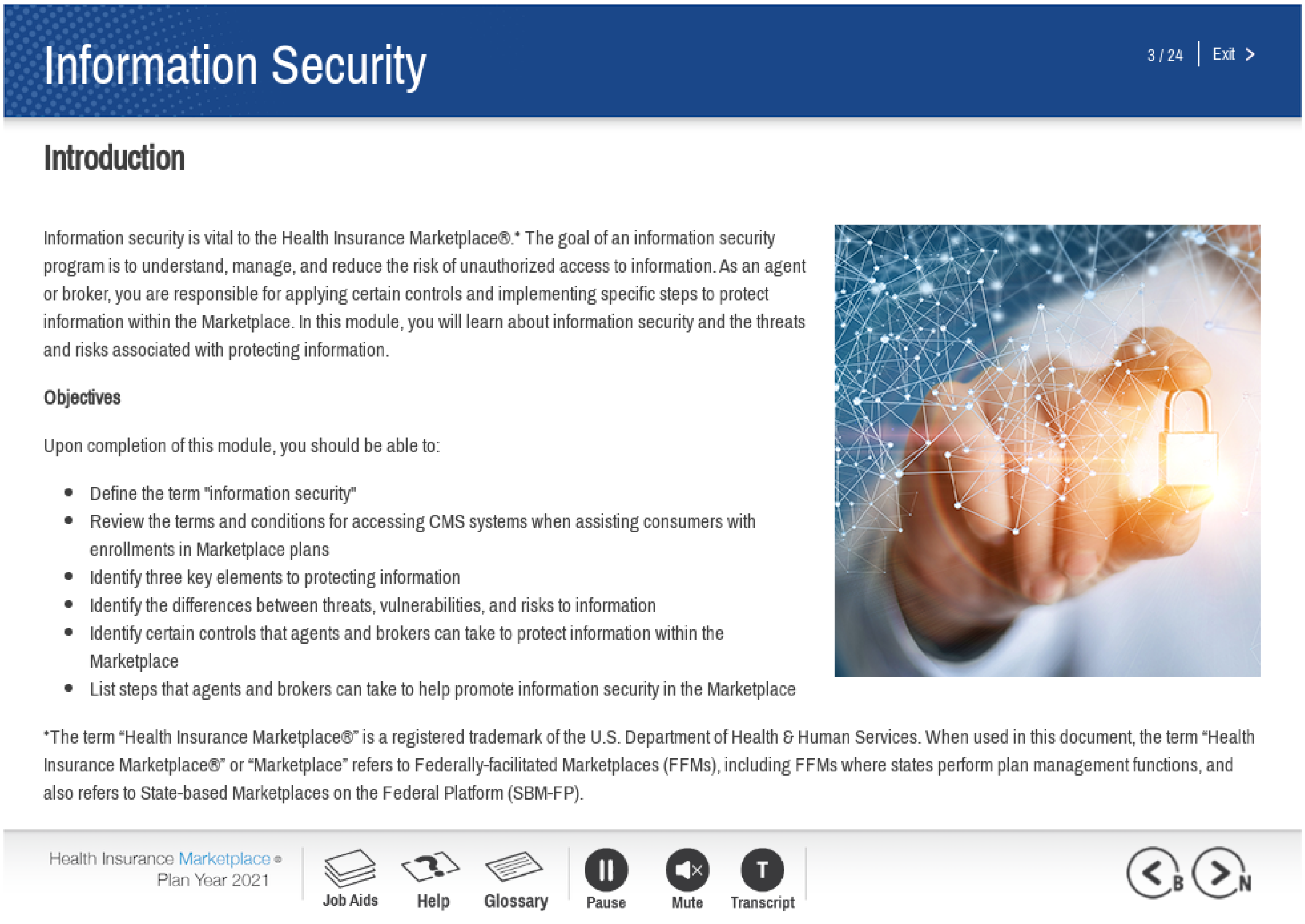
The information in this training was current at the time it was published or uploaded onto the Web. Eligibility policies and Marketplace requirements may change so links to the source documents have been provided within the document for your reference. This training is not intended to grant rights or 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

Page: 3 of 24: Introduction



Information Security

Introduction

Information security is vital to the Health Insurance 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 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"
- Review the terms and conditions for accessing CMS systems when assisting consumers with enrollments in Marketplace plans
- 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 Marketplace
- List steps that agents and brokers can take to help promote information security in the Marketplace

*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 (FFMs), including FFMs where states perform plan management functions, and also refers to State-based Marketplaces on the Federal Platform (SBM-FP).

Page Text

Information security is vital to the Health Insurance 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 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:

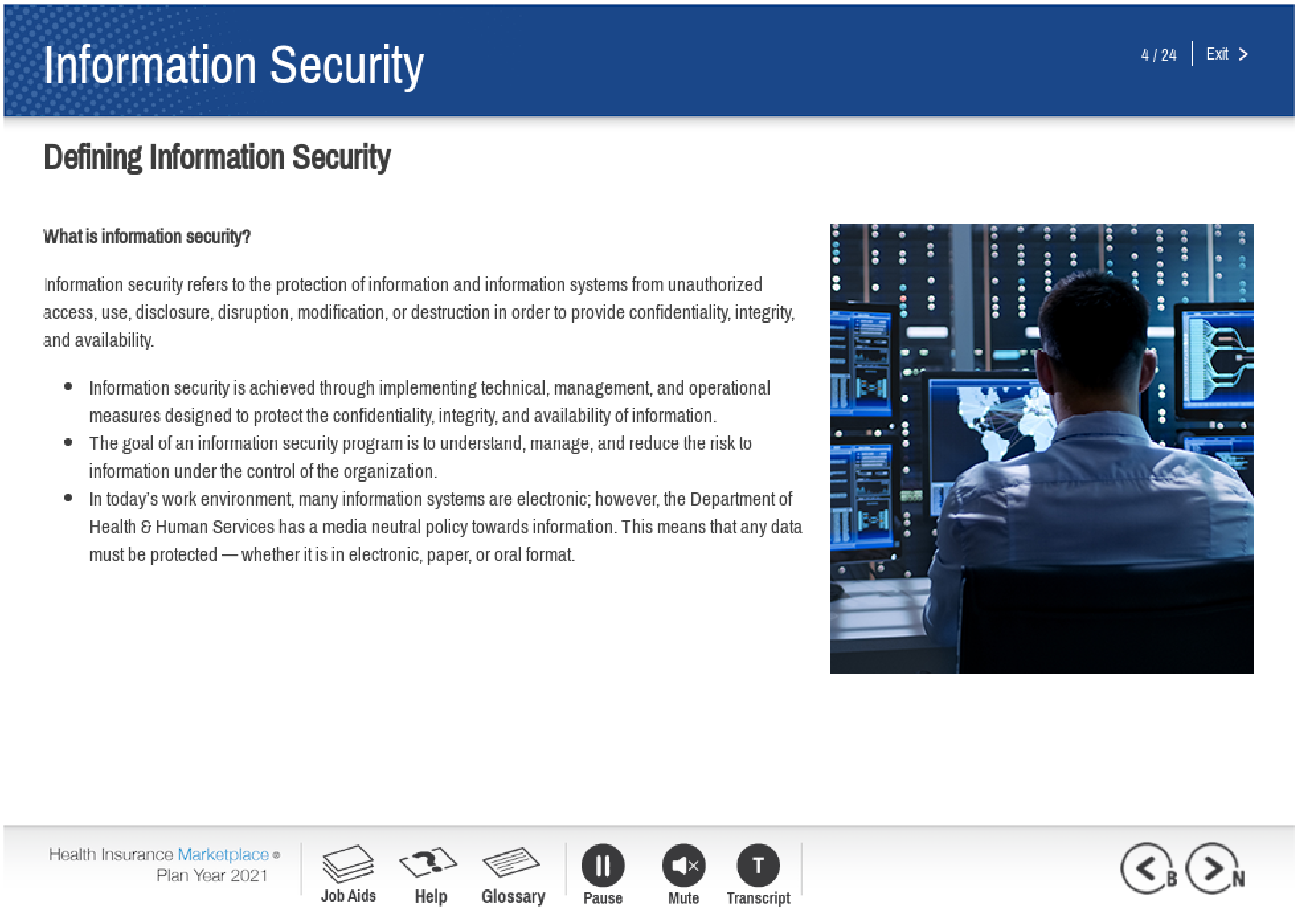
- Define the term "information security"
- Review the terms and conditions for accessing CMS systems when assisting consumers with enrollments in Marketplace plans
- Identify three key elements to protecting information
- Identify the differences between threats, vulnerabilities, and risks to information
- Identify certain controls that agents and brokers can take to protect information within the Marketplace
- List steps that agents and brokers can take to help promote information security in the Marketplace

*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 (FFMs), including FFMs where states perform plan management functions, and also refers to State-based Marketplaces on the Federal Platform (SBM-FP).

Alt Text

A person holding a small gold, glowing padlock with connecting lines coming from it

Page: 4 of 24: Defining Information Security



Information Security

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

Page Text

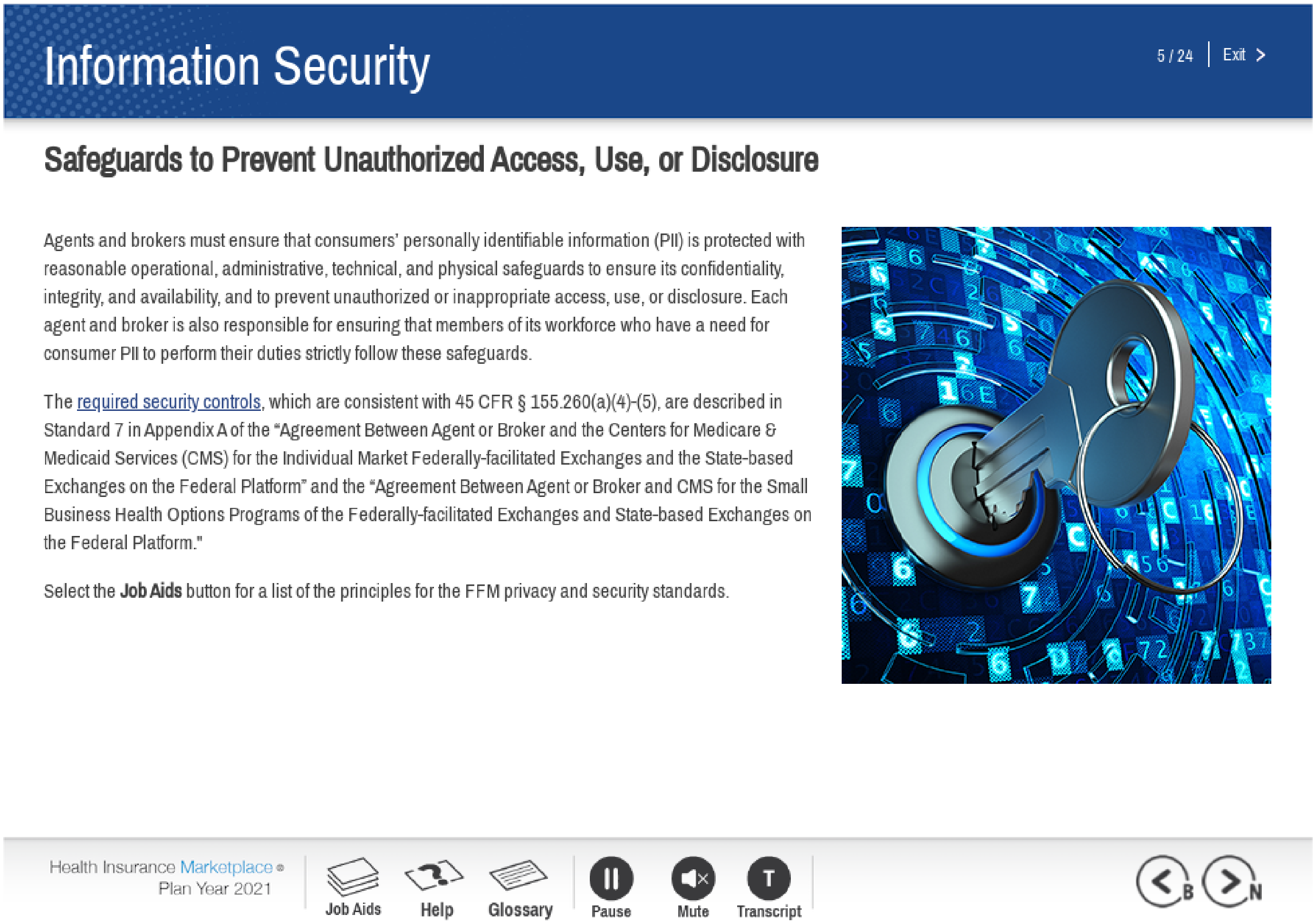
What is information security? Information security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

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

Alt Text

A person sitting in an analysis room viewing multiple computer screens

Page: 5 of 24: Safeguards to Prevent Unauthorized Access, Use, or Disclosure



Safeguards to Prevent Unauthorized Access, Use, or Disclosure

Agents and brokers must ensure that consumers' personally identifiable information (PII) is 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. Each agent and broker is also responsible for ensuring that members of its workforce who have a need for consumer PII to perform their duties strictly follow these safeguards.

The required security controls, which are consistent with 45 CFR § 155.260(a)(4)-(5), are described in Standard 7 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" and the "Agreement Between Agent or Broker and CMS for the Small Business Health Options Programs of the Federally-facilitated Exchanges and State-based Exchanges on the Federal Platform."

Select the **Job Aids** button for a list of the principles for the FFM privacy and security standards.

Page Text

Agents and brokers must ensure that consumers' personally identifiable information (PII) is 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. Each agent and broker is also responsible for ensuring that members of its workforce who have a need for consumer PII to perform their duties strictly follow these safeguards. The required security controls, which are consistent with 45 CFR § 155.260(a)(4)-(5), are described in Standard 7 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" and the "Agreement Between Agent or Broker and CMS for the Small Business Health Options Programs of the Federally-facilitated Exchanges and State-based Exchanges on the Federal Platform." Select the Job Aids button for a list of the principles for the FFM privacy and security standards.

Alt Text

A key inserted into a keyhole; numbers surround the keyhole in a circular fashion.

Required Security Controls Pop Up text:

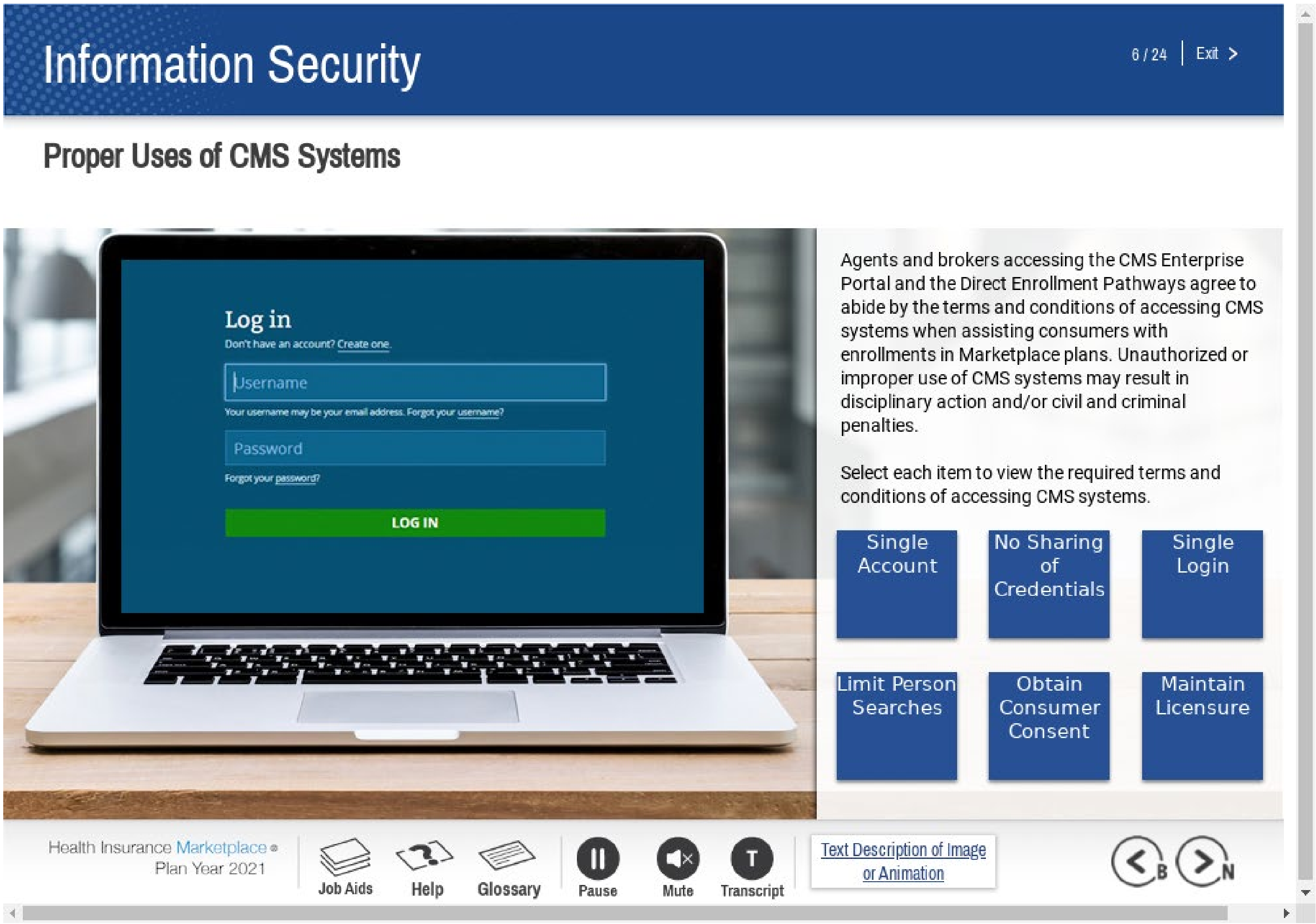
The required security controls must ensure that:

- PII is only used by or disclosed to those authorized to receive or view it;

- PII is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information;
- PII is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law; and
- PII is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules.

Agents and brokers must monitor, periodically assess, and update their security controls and related system risks to ensure the continued effectiveness of those controls. They must also develop and utilize secure electronic interfaces when transmitting PII electronically.

Page: 6 of 24: Proper Uses of CMS Systems



Information Security

6 / 24 | Exit >

Proper Uses of CMS Systems

Agents and brokers accessing the CMS Enterprise Portal and the Direct Enrollment Pathways agree to abide by the terms and conditions of accessing CMS systems when assisting consumers with enrollments in Marketplace plans. Unauthorized or improper use of CMS systems may result in disciplinary action and/or civil and criminal penalties.

Select each item to view the required terms and conditions of accessing CMS systems.

Log in
Don't have an account? Create one.
Username
Your username may be your email address. Forgot your username?
Password
Forgot your password?
LOG IN
Single Account
No Sharing of Credentials
Single Login
Limit Person Searches
Obtain Consumer Consent
Maintain Licensure
Health Insurance Marketplace Plan Year 2021
Job Aids
Help
Glossary
Pause
Mute
Transcript
Text Description of Image or Animation
B
N

Long Description

Interactive graphic: to the left of the screen is a laptop with the login screen for HealthCare.gov displayed.

To the right of the screen is the following text:

Agents and brokers accessing the CMS Enterprise Portal and the Direct Enrollment Pathways agree to abide by the terms and conditions of accessing CMS systems when assisting consumers with enrollments in Marketplace plans. Unauthorized or improper use of CMS systems may result in disciplinary action and/or civil and criminal penalties.

Prompt text: Select each item to view the required terms and conditions of accessing CMS systems.

Below the prompt text are six squares labeled with the following:

Single Account, No Sharing of Credentials, Single Login, Limit Person Searches, Obtain Consumer Consent, Maintain Licensure

When each square is selected, a popup box is displayed with accompanying text.

Single Account Pop Up text:
Individuals are allowed to have only one CMS Portal account.

No Sharing of Credentials Pop Up text:

- Only the person creating a CMS Portal account may use his or her log-in credentials. Sharing log-in credentials is not allowed.
- Agents and brokers may not log in to HealthCare.gov on a consumer's behalf (i.e., using the consumer's HealthCare.gov ID and password).

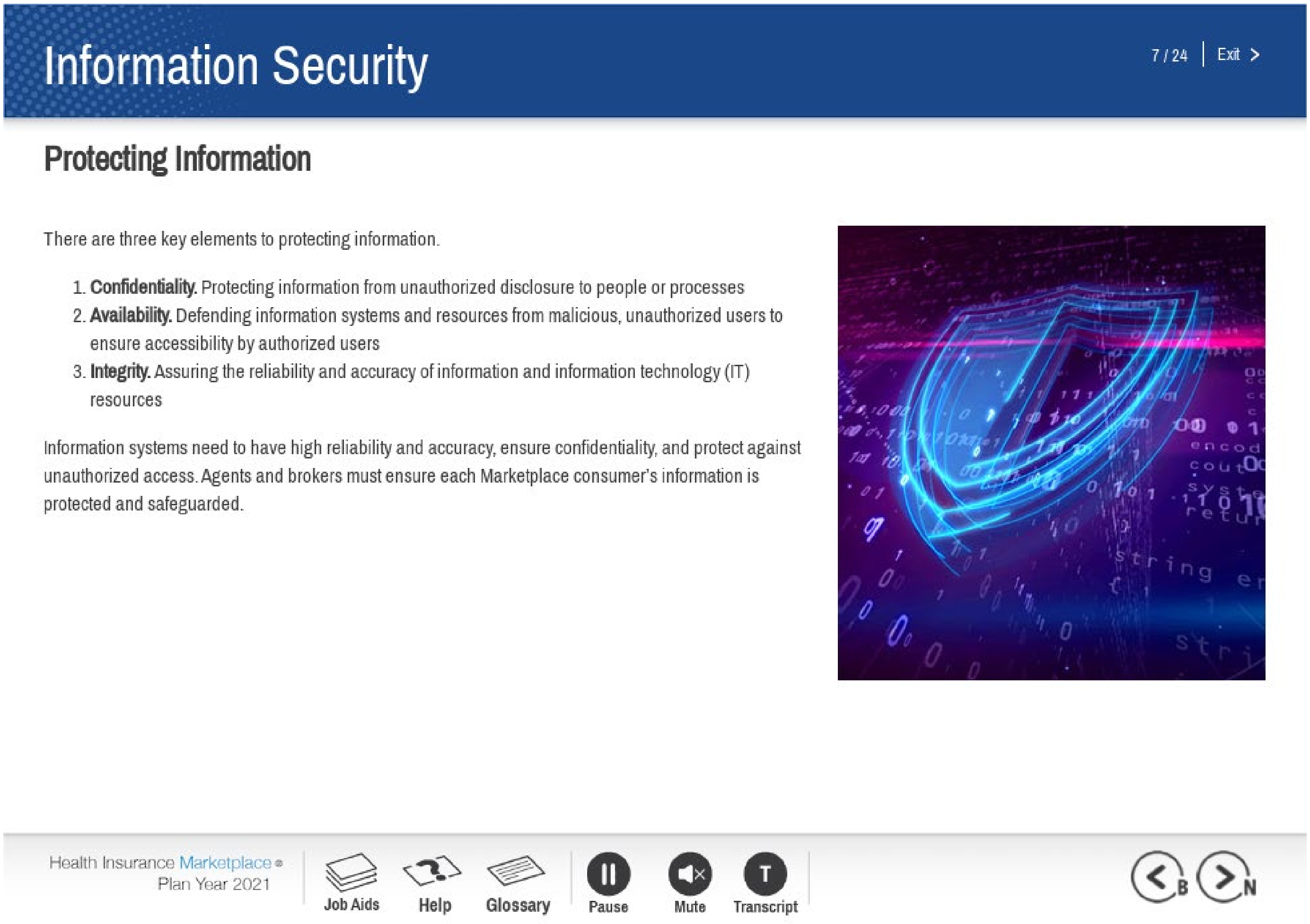
Single Login Pop Up text:
An agent or broker may log in to his or her CMS Portal account with a single login session and conduct person searches and any other electronic searches through the Direct Enrollment Pathways. If you are logged in and then try to log in again with a new browser window, tab, or other computer, your first session will end. This system check will effectively prevent multiple people from using the same login credentials.

Limit Person Searches Pop Up text:
Users may conduct only one person search at a time during a log in session. Use of scripts and other automation of interactions with CMS Systems or the Direct Enrollment Pathways are strictly prohibited, unless approved in advance in writing by CMS. Users conduct automated activities may have their CMS Portal accounts disabled immediately and without prior notice. This does not apply to scripted interactions with public-facing application programming interfaces maintained by CMS.

Obtain Consumer Consent Pop Up text:
Agents and brokers may only conduct person searches for consumers who have given their consent to assist them with applying for and enrolling in a Marketplace plan. As a best practice, CMS recommends getting this consent in writing. If you have worked with a client in the past and the prior consent has been revoked or otherwise terminated, you should receive consent from that client again to conduct a person search in connection with enrollment in a Marketplace plan. Conducting person searches for non-Marketplace enrollment purposes (e.g., to enroll the person in a non-Marketplace plan) is not allowed and may result in CMS Portal account suspension and subsequent termination of the agent’s or broker’s applicable Marketplace Agreements and FFM registration.

Maintain Licensure Pop Up text:
Agents and brokers wanting to assist consumers with Marketplace enrollment through HealthCare.gov or any Direct Enrollment Pathway (Classic or Enhanced) must be licensed in each state where they are assisting consumers. Agents and brokers must undergo identity proofing, complete required training, and sign applicable Agreements with the Marketplace for the applicable benefit year prior to assisting Marketplace consumers. CMS will disable access to the CMS Portal and the Direct Enrollment Pathways for any agent or broker where CMS is unable to verify state health insurance licensure using the National Insurance Producer Registry and may subsequently terminate the agent’s or broker’s Marketplace Agreements and FFM registration.

Page: 7 of 24: Protecting Information



Information Security

7 / 24 | Exit >

Protecting Information

There are three key elements to protecting information.

1. **Confidentiality.** Protecting information from unauthorized disclosure to people or processes
2. **Availability.** Defending information systems and resources from malicious, unauthorized users to ensure accessibility by authorized users
3. **Integrity.** Assuring the reliability and accuracy of information and information technology (IT) resources

Information systems need to have high reliability and accuracy, ensure confidentiality, and protect against unauthorized access. Agents and brokers must ensure each Marketplace consumer's information is protected and safeguarded.

Page Text

There are three key elements to protecting information.

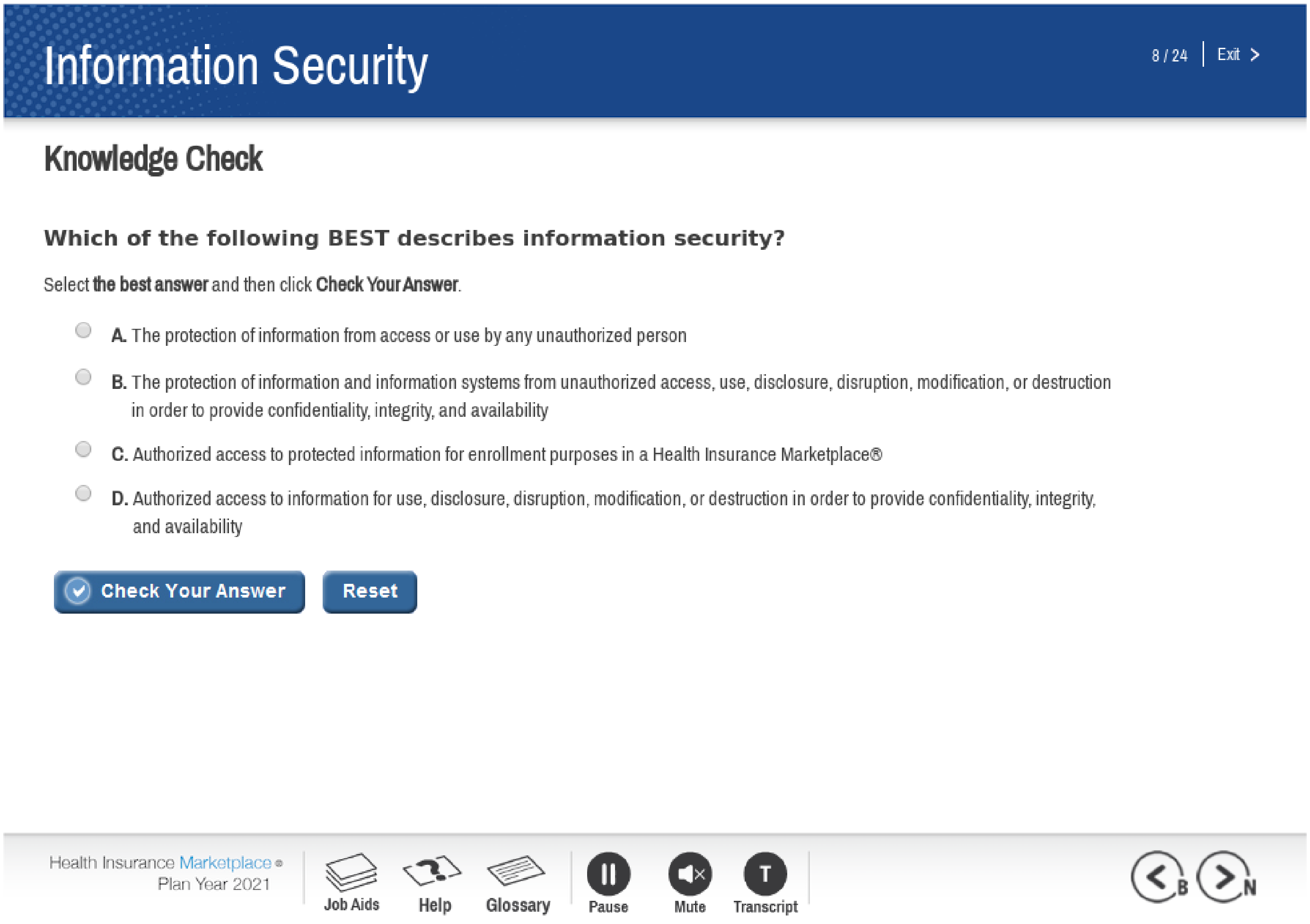
- Confidentiality. Protecting information from unauthorized disclosure to people or processes
- Availability. Defending information systems and resources from malicious, unauthorized users to ensure accessibility by authorized users
- Integrity. Assuring the reliability and accuracy of information and information technology (IT) resources

Information systems need to have high reliability and accuracy, ensure confidentiality, and protect against unauthorized access. Agents and brokers must ensure each Marketplace consumer's information is protected and safeguarded.

Alt Text

A conceptual illustration of a shield over a field of computer code representing information security.

Page: 8 of 24: Knowledge Check



Information Security

Knowledge Check

Which of the following BEST describes information security?

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

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

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

○ **C.** Authorized access to protected information for enrollment purposes in a Health Insurance Marketplace®

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

Prompt

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

Question

Which of the following BEST describes information security?

Options

A. The protection of information from access or use by any unauthorized person
B. The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability
C. Authorized access to protected information for enrollment purposes in a Health Insurance Marketplace®
D. Authorized access to information for use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability

Correct Answer

B

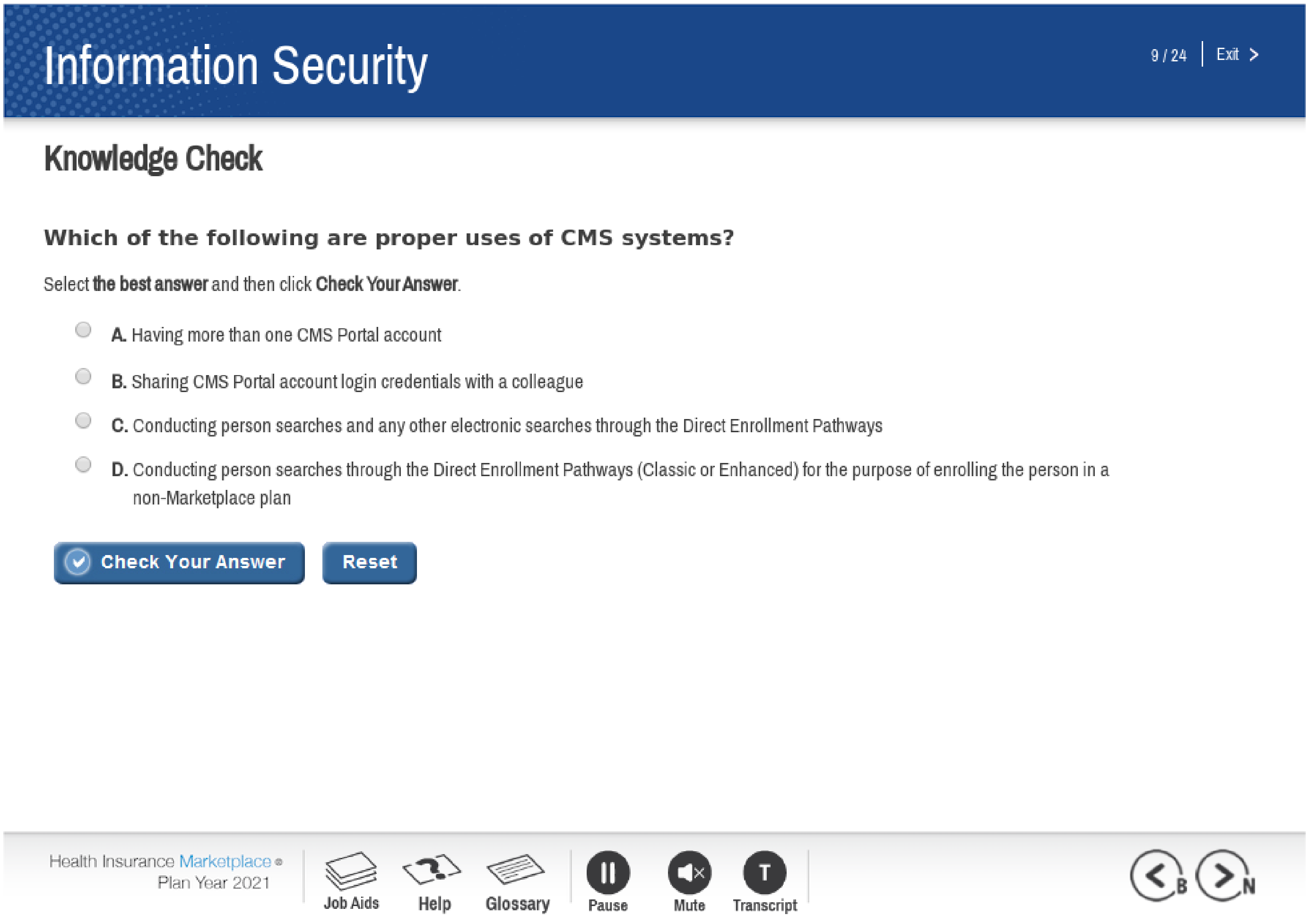
Positive Feedback

Correct! 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.

Negative Feedback

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

Page: 9 of 24: Knowledge Check



Knowledge Check

Which of the following are proper uses of CMS systems?

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

○ **A.** Having more than one CMS Portal account

○ **B.** Sharing CMS Portal account login credentials with a colleague

○ **C.** Conducting person searches and any other electronic searches through the Direct Enrollment Pathways

○ **D.** Conducting person searches through the Direct Enrollment Pathways (Classic or Enhanced) for the purpose of enrolling the person in a non-Marketplace plan

Prompt

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

Question

Which of the following are proper uses of CMS systems?

Options

A. Having more than one CMS Portal account
B. Sharing CMS Portal account login credentials with a colleague
C. Conducting person searches and any other electronic searches through the Direct Enrollment Pathways
D. Conducting person searches through the Direct Enrollment Pathways (Classic or Enhanced) for the purpose of enrolling the person in a non-Marketplace plan

Correct Answer

C

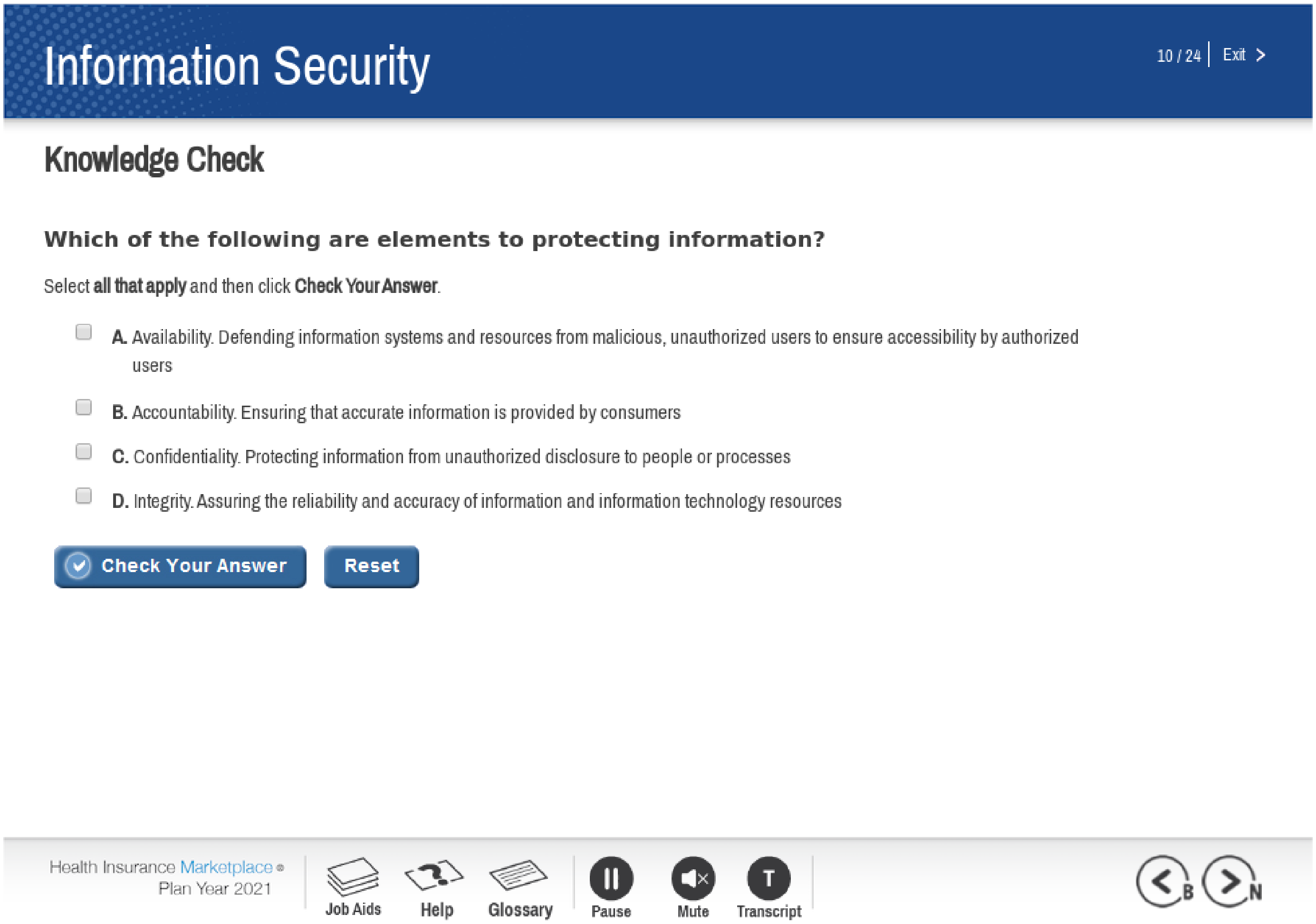
Positive Feedback

Correct! Users may conduct only one person search at a time. Individuals are allowed to have only one CMS Portal account and may not share the login credentials for that account with anyone. Conducting person searches for non-Marketplace enrollment purposes (e.g., to enroll an individual in a non-Marketplace plan) is not allowed.

Negative Feedback

Incorrect. The correct answer is C. Users may conduct only one person search at a time. Individuals are allowed to have only one CMS Portal account and may not share the login credentials for that account with anyone. Conducting person searches for non-Marketplace enrollment purposes (e.g., to enroll an individual in a non-Marketplace plan) is not allowed.

Page: 10 of 24: Knowledge Check



Knowledge Check

Which of the following are elements to protecting information?

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

□ **A.** Availability. Defending information systems and resources from malicious, unauthorized users to ensure accessibility by authorized users

□ **B.** Accountability. Ensuring that accurate information is provided by consumers

□ **C.** Confidentiality. Protecting information from unauthorized disclosure to people or processes

□ **D.** Integrity. Assuring the reliability and accuracy of information and information technology resources

Prompt

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

Question

Which of the following are elements to protecting information?

Options

A. Availability. Defending information systems and resources from malicious, unauthorized users to ensure accessibility by authorized users
B. Accountability. Ensuring that accurate information is provided by consumers
C. Confidentiality. Protecting information from unauthorized disclosure to people or processes
D. Integrity. Assuring the reliability and accuracy of information and information technology resources

Correct Answer

A, C, D

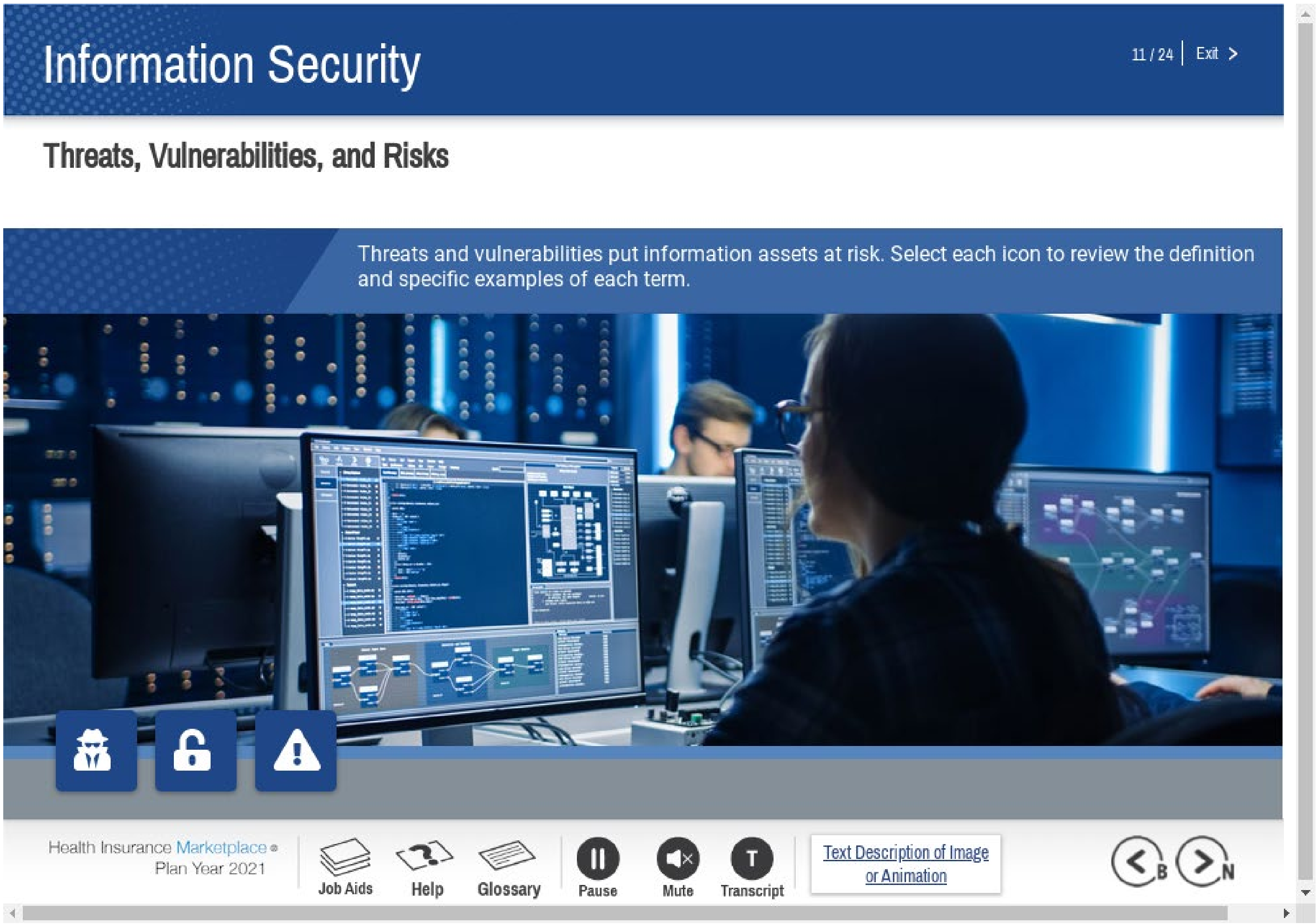
Positive Feedback

Correct! Availability, confidentiality, and integrity are the three key elements to protecting information.

Negative Feedback

Incorrect. The correct answers are A, C, and D. Availability, confidentiality, and integrity are the three key elements to protecting information.

Page: 11 of 24: Threats, Vulnerabilities, and Risks



Information Security

Threats, Vulnerabilities, and Risks

Threats and vulnerabilities put information assets at risk. Select each icon to review the definition and specific examples of each term.

11 / 24
Exit
Health Insurance Marketplace
Plan Year 2021
Job Aids
Help
Glossary
Pause
Mute
Transcript
Text Description of Image or Animation
B
N

Long Description

Interactive graphic of three icons lined up at the bottom of the screen. When each icon is selected, associated text appears in the middle of the screen. The main image is of a woman working in a Secure Compartmented Information Facility (SCIF).

Prompt:
Threats and vulnerabilities put information assets at risk. Select each icon to review the definition and specific examples of each term.

The following text is shown in the middle of the screen when an icon is selected from left to right:

Threat image: man wearing a trench coat, sunglasses and a hat
Threat Pop Up text:
A threat is the potential to cause unauthorized disclosure, changes to, or destruction of an asset. Impacts can include:

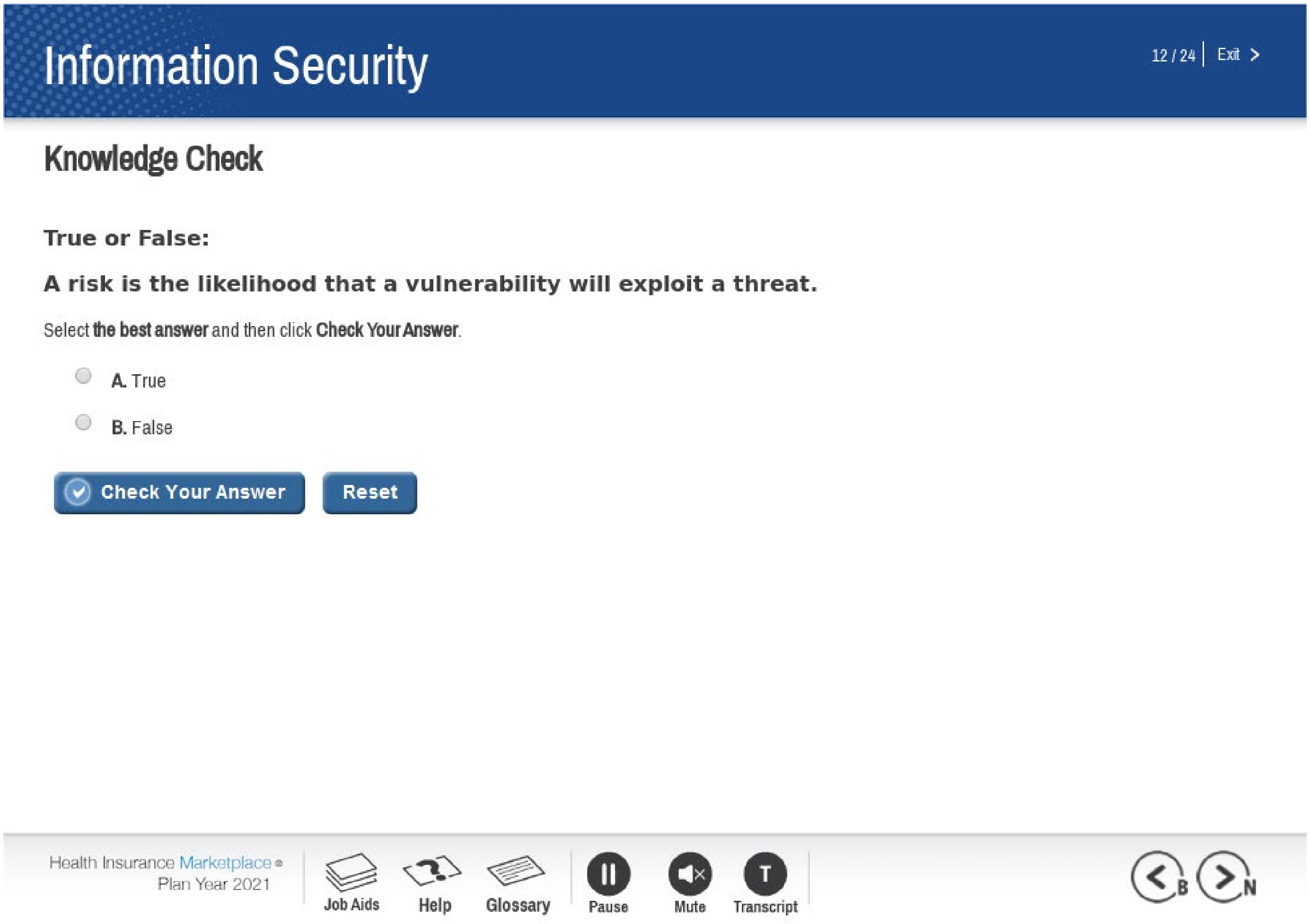
- Potential breach in confidentiality
- Potential breach in integrity
- Unavailability of information
- Types of threats:
- Natural
- Environmental
- Man-made

Vulnerability image: a padlock
Vulnerability Pop Up text:
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. Examples of vulnerabilities include:

- Poor standards for creating usernames and passwords
- Flaws in computer software

Risk image: a triangle with an exclamation point in the center
Risk image Pop Up text:
A risk is the likelihood that a threat will exploit a vulnerability. An example of a risk is a system that 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.

Page: 12 of 24: Knowledge Check



Information Security

12 / 24 | Exit >

Knowledge Check

True or False:

A risk is the likelihood that a vulnerability will exploit a threat.

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

○ **A.** True

○ **B.** False

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

Question
True or False: A risk is the likelihood that a vulnerability will exploit a threat.

Options
A. True
B. False

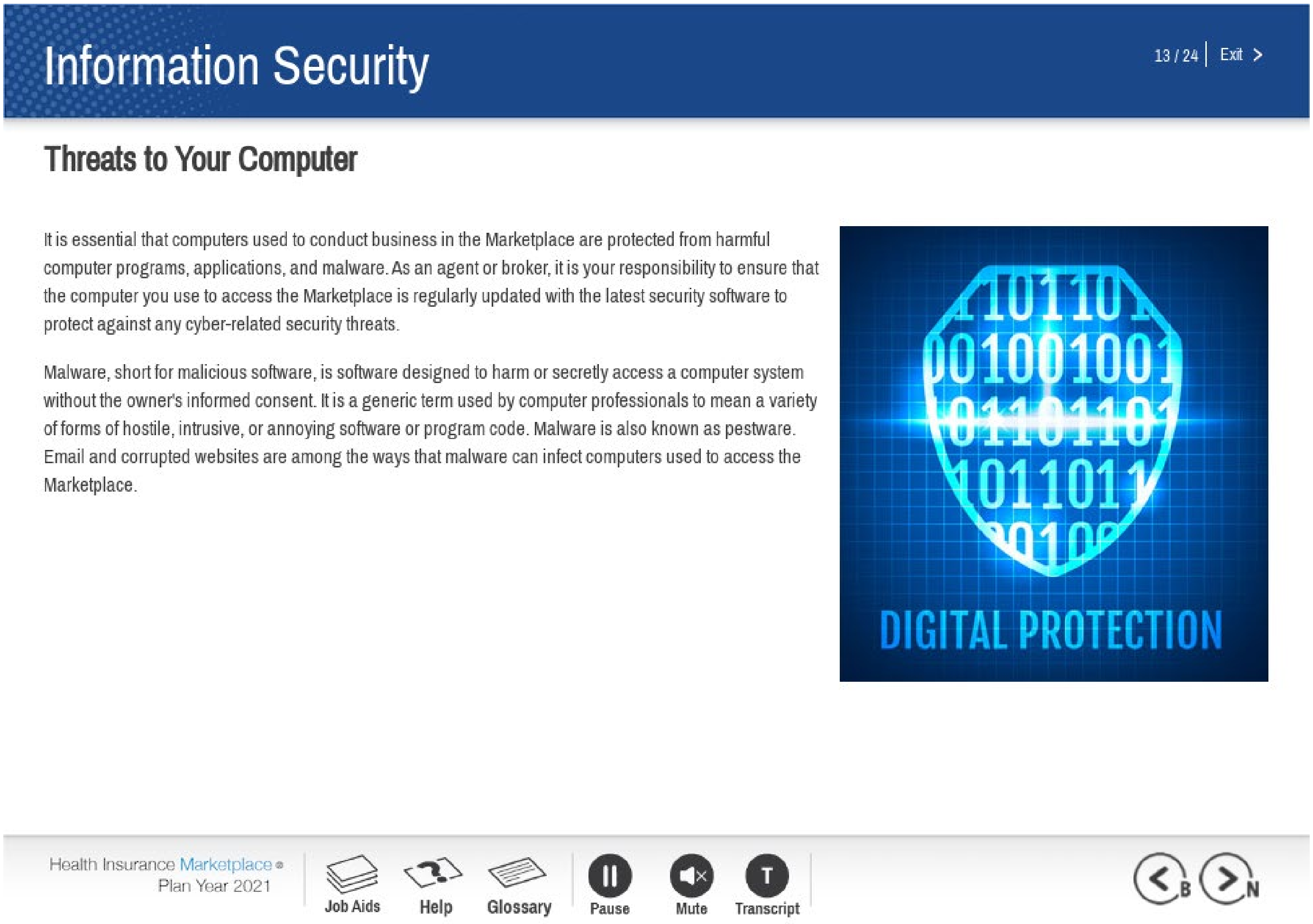
Correct Answer
B

Positive Feedback
Correct. 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. A threat is the potential to cause unauthorized disclosure, changes to, or destruction of an asset. 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.

Negative Feedback

Incorrect. The statement is false. 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. A threat is the potential to cause unauthorized disclosure, changes to, or destruction of an asset. 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.

Page: 13 of 24: Threats to Your Computer



Information Security

13 / 24 | Exit >

Threats to Your Computer

It is essential that computers used to conduct business in the 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 the 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 Marketplace.

Page Text

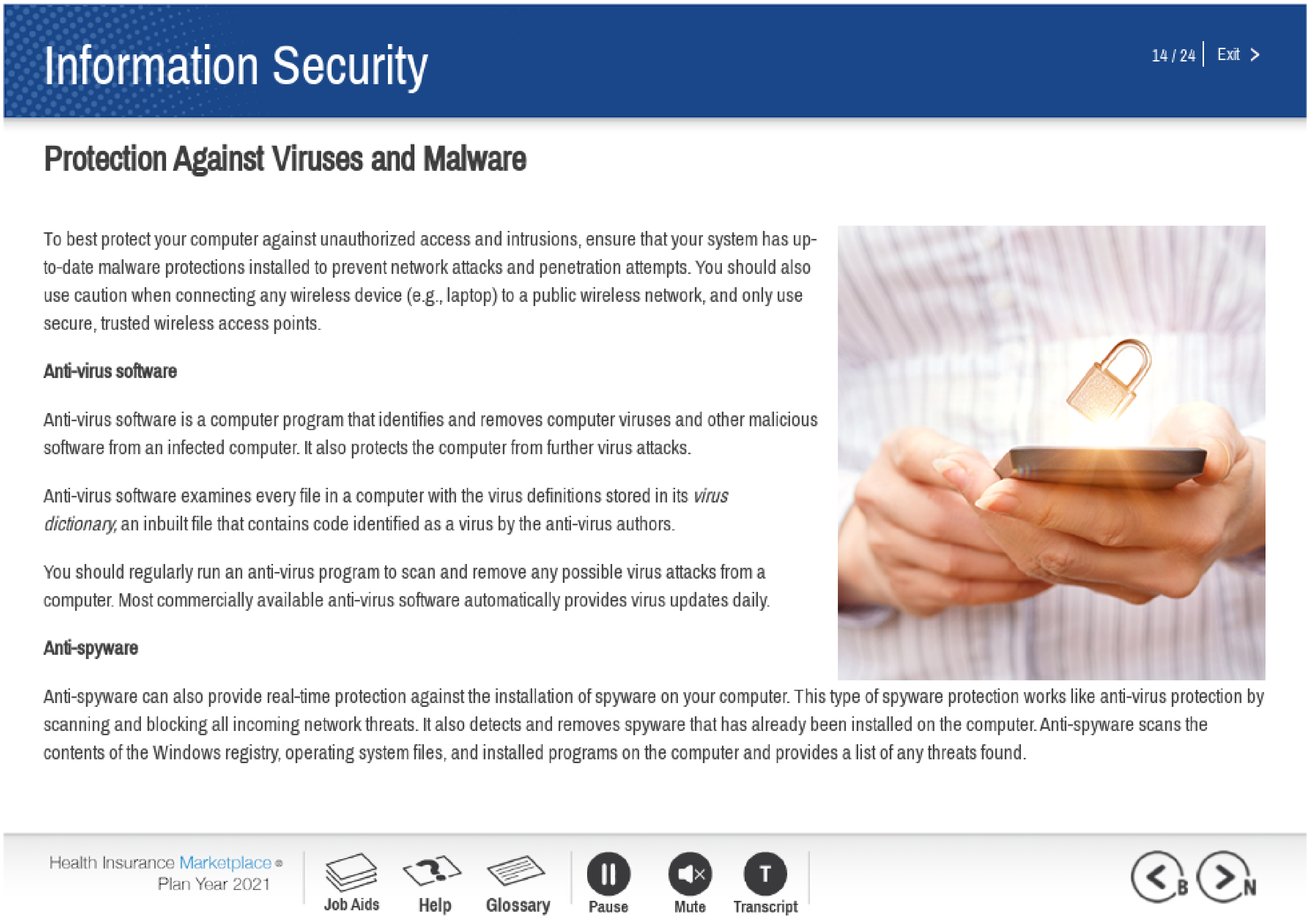
It is essential that computers used to conduct business in the Marketplace are protected from harmful computer programs, applications, and malware. As an agent or broker, it is your responsibility to ensure that the computer you use to access the Marketplace is regularly updated with the latest security 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 Marketplace.

Alt Text

A blue shield with numbers 00100100 repeated on the shield. Underneath the shield are the words Digital Protection.

Page: 14 of 24: Protection Against Viruses and Malware



Protection Against Viruses and Malware

To best protect your computer against unauthorized access and intrusions, ensure that your system has up-to-date malware protections installed to prevent network attacks and penetration attempts. You should also use caution when connecting any wireless device (e.g., laptop) to a public wireless network, and only use secure, trusted wireless access points.

Anti-virus software

Anti-virus software is a computer program that identifies and removes computer viruses and other malicious software 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 on 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.

Page Text

To best protect your computer against unauthorized access and intrusions, ensure that your system has up-to-date malware protections installed to prevent network attacks and penetration attempts. You should also use caution when connecting any wireless device (e.g., laptop) to a public wireless network, and only use secure, trusted wireless access points.

Anti-virus software

Anti-virus software is a computer program that identifies and removes computer viruses and other malicious software 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.

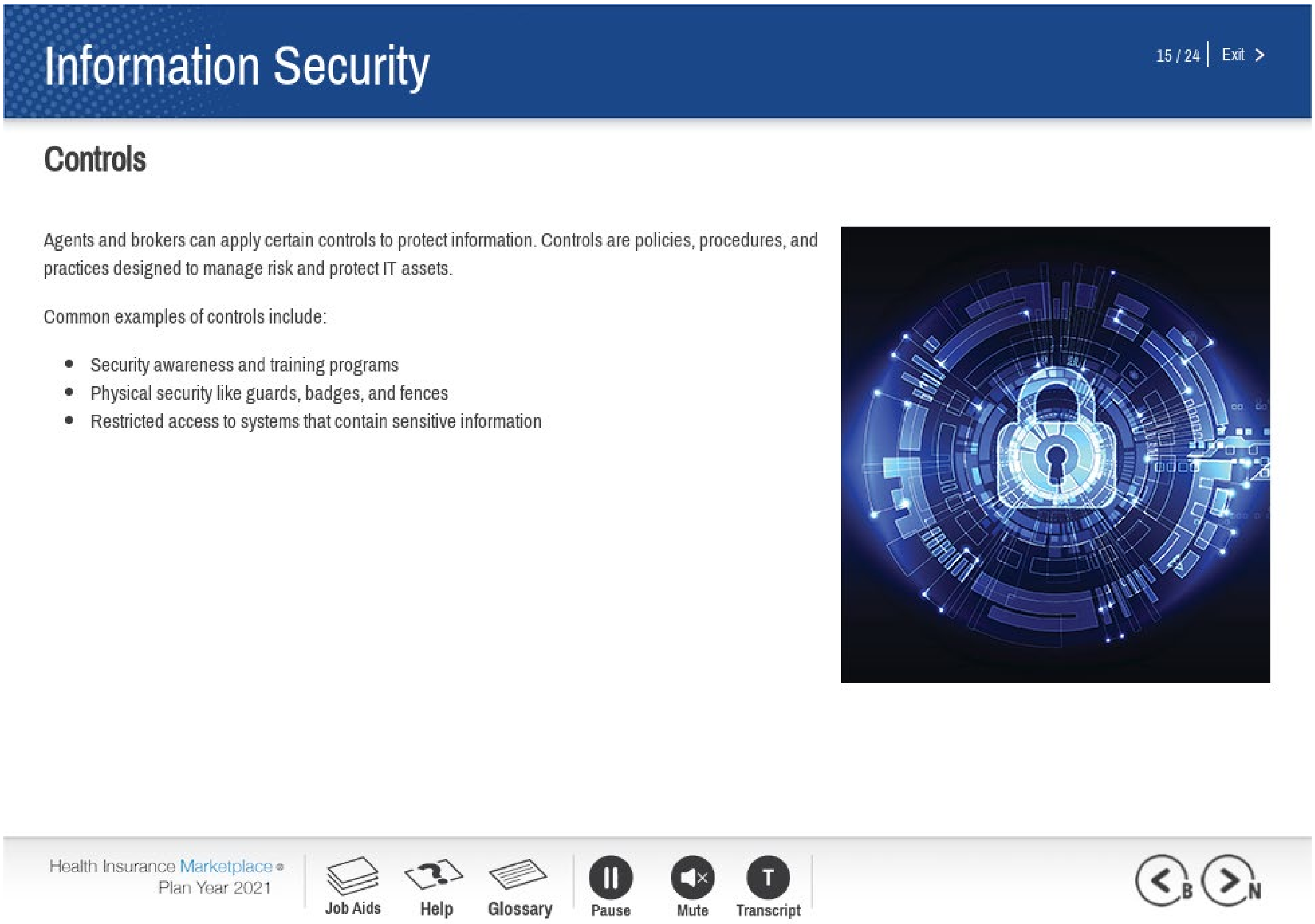
Anti-spyware

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 on 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.

Alt Text

Close-up image of a person holding phone that is glowing; a padlock is levitating above the phone screen.

Page: 15 of 24: Controls



Information Security

Controls

Agents and brokers can apply certain controls to protect information. 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
- Restricted access to systems that contain sensitive information

Page Text

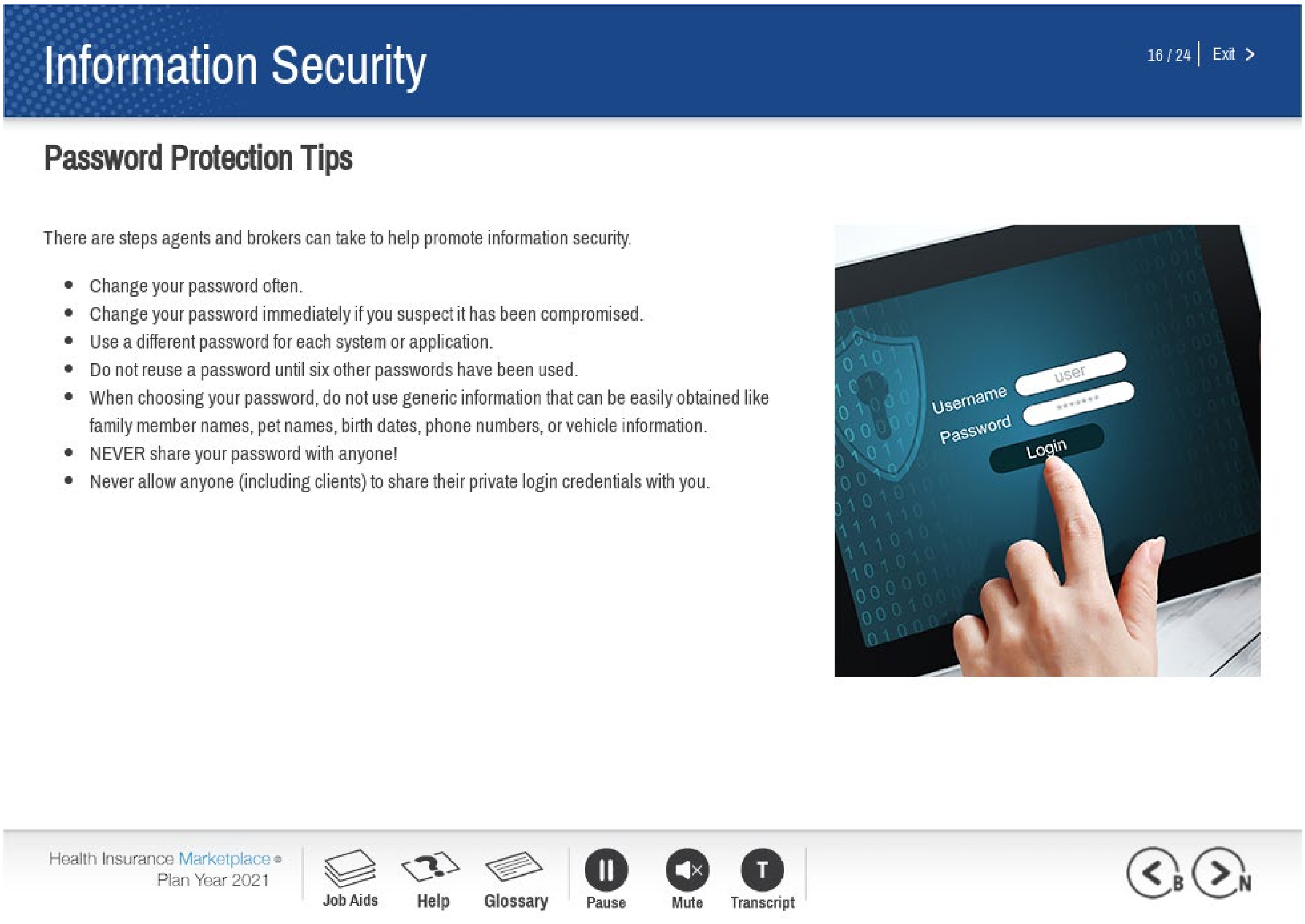
Agents and brokers can apply certain controls to protect information. Controls are policies, procedures, and practices designed to manage risk and protect IT assets. Common examples of controls include:

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

Alt Text

A padlock surrounded by circles

Page: 16 of 24: Password Protection Tips



Information Security

16 / 24 | Exit >

Password Protection Tips

There are steps agents and brokers can take to help promote information security.

- 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!
- Never allow anyone (including clients) to share their private login credentials with you.

Page Text

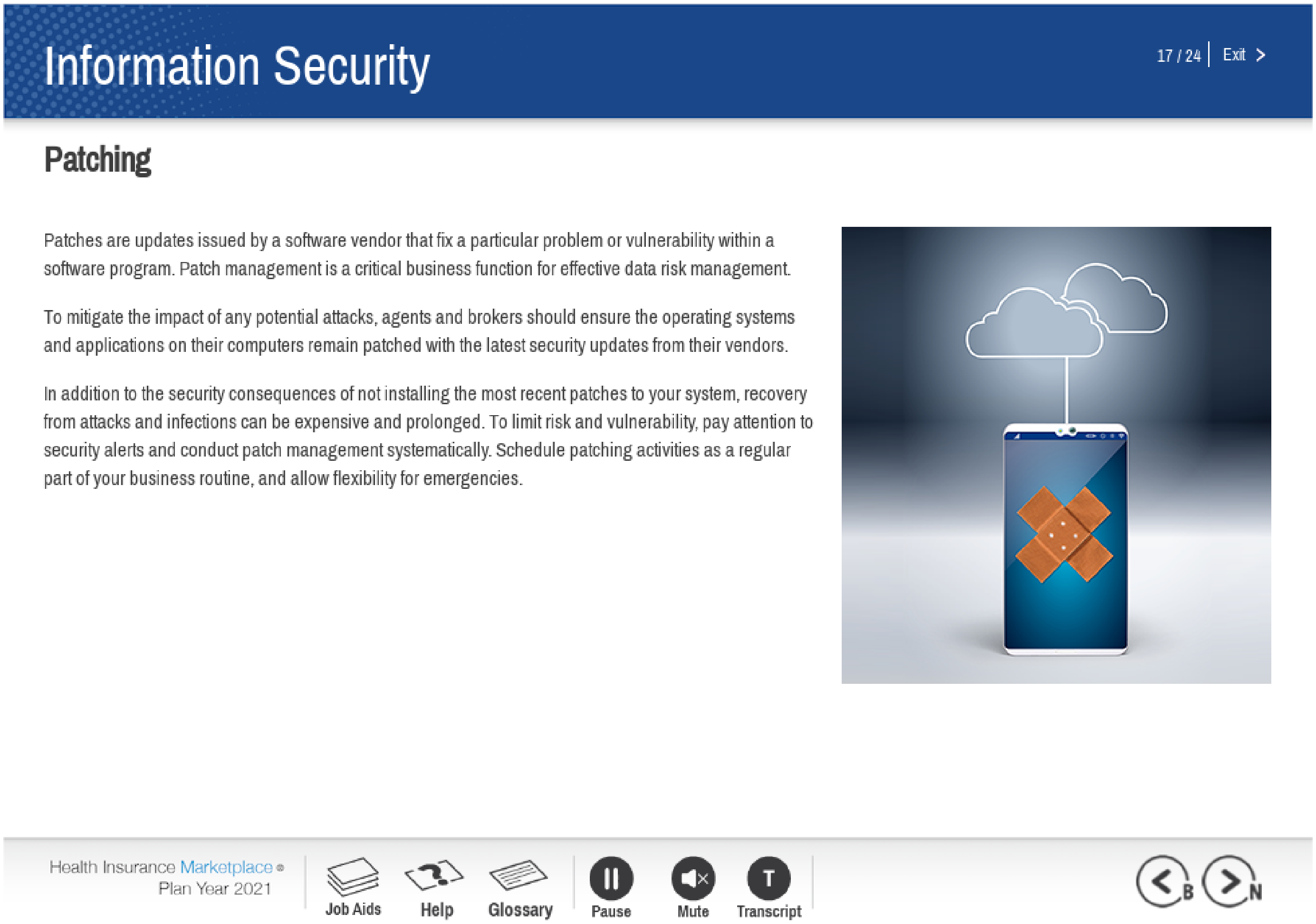
There are steps agents and brokers can take to help promote information security.

- 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!
- Never allow anyone (including clients) to share their private login credentials with you.

Alt Text

A computer screen with Username and Password buttons and enter fields stacked on top of each other. 'Username': 'User' displayed; 'Password': '*****' displayed; a finger pointing to a button that reads 'Login'; a shield with code in vertical rows to the left of the buttons.

Page: 17 of 24: Patching



Information Security

Patching

Patches are updates issued by a software 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.

Page Text

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

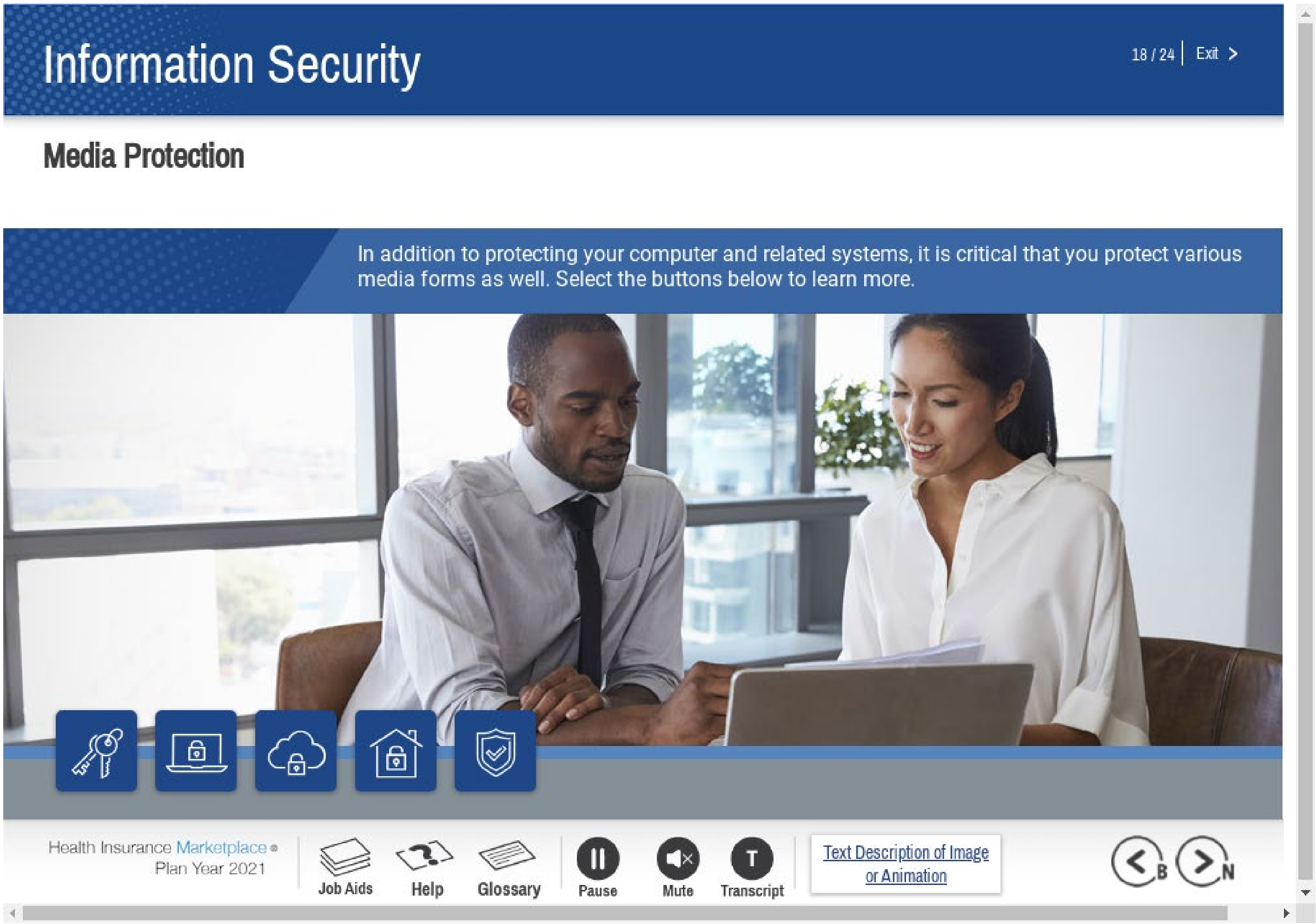
To mitigate the impact of any potential attacks, agents and brokers should ensure the operating systems and applications on their computers remain patched with the latest security updates from their vendors.

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.

Alt Text

Phone with two band aids displayed that form a cross; two clouds are hovering over the phone connected by a line

Page: 18 of 24: Media Protection



In addition to protecting your computer and related systems, it is critical that you protect various media forms as well. Select the buttons below to learn more.

Long Description

Interactive graphic showing two people gathered around a conference room table and looking at a computer. At the bottom left of the graphic are five buttons, each with a different animated icon. From left to right the icons are: a set of keys, a computer screen displaying a padlock, a padlock surrounded by a cloud, a house with a padlock in the center of it, and a shield with a check mark in the center of it. When the icons are selected a pop-up box displays with accompanying text.

The top of the graphic displays the following prompt text: In addition to protecting your computer and related systems, it is critical that you protect various media forms as well. Select the buttons below to learn more.

Set of Keys Pop Up text:
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 machine receiving the document is not in a public area and that the individual receiving the fax is aware it is being sent and confirms receipt.

Computer screen displaying a padlock Pop Up text:
Protect Your Equipment:
Mobile computing devices (e.g., phones, laptops, portable storage devices, thumb drives) should be secured by way of appropriate locks or other safeguards to protect from theft. Always discard consumer PII through shredding or secured refuse removal.

Padlock surrounded by a cloud Pop Up text:
Protect Email and Conversations:
Ensure communications are encrypted when exchanging PII or other sensitive data electronically. Encryption protects the confidentiality of the email by scrambling the message, thus requiring a password to decrypt the message. Encrypting email attachments also protects them from being compromised on unencrypted servers. Sending passwords via email is not recommended. At a minimum, do not send the password in the same email as the encrypted file. Suggested methods of password transmittal include text message, phone conversation, predetermined shared secrets, or a shared file system (e.g., SharePoint®).

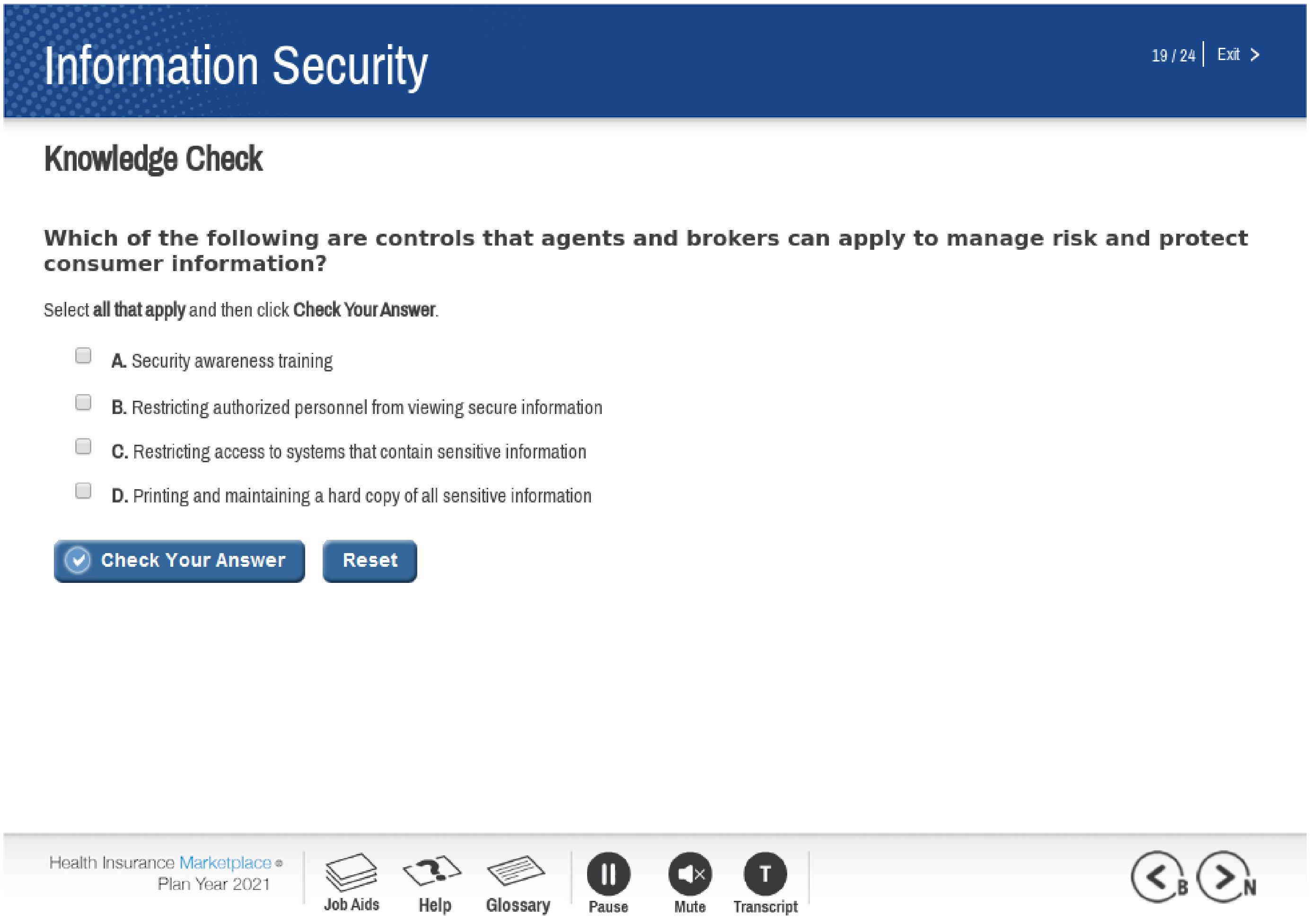
A predetermined shared secret is the most practical for sharing information with large groups. An example of a predetermined shared secret would be a password that is established in person during a group meeting or another secure channel and shared before it needs to be used. Only the parties involved in the group meeting or with access to the other secure channel would know the password, and only those parties could use the password to open an encrypted file. 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 other forms of mass transit.

House with a padlock in the center of it Pop Up text:
Protect Your Area:
Recognize, politely challenge, and assist people who do not belong in the work area to avoid potential security attacks. 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 to areas where there are information systems that contain consumer PII should be restricted to authorized persons.
- 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. Utilize privacy filter screens as necessary.

Shield with a checkmark in the center of it Pop Up text:
Protect Sensitive Unclassified Information:
Disclosure and modification of a consumer's PII that is not specifically authorized is prohibited. This data (including PII) should not be used for unauthorized or illegal purposes, for private gain, or to misrepresent oneself or the federal government.

Page: 19 of 24: Knowledge Check



Knowledge Check

Which of the following are controls that agents and brokers can apply to manage risk and protect consumer information?

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

□ **A.** Security awareness training

□ **B.** Restricting authorized personnel from viewing secure information

□ **C.** Restricting access to systems that contain sensitive information

□ **D.** Printing and maintaining a hard copy of all sensitive information

Prompt

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

Question

Which of the following are controls that agents and brokers can apply to manage risk and protect consumer information?

Options

A. Security awareness training
B. Restricting authorized personnel from viewing secure information
C. Restricting access to systems that contain sensitive information
D. Printing and maintaining a hard copy of all sensitive information

Correct Answer

A, C

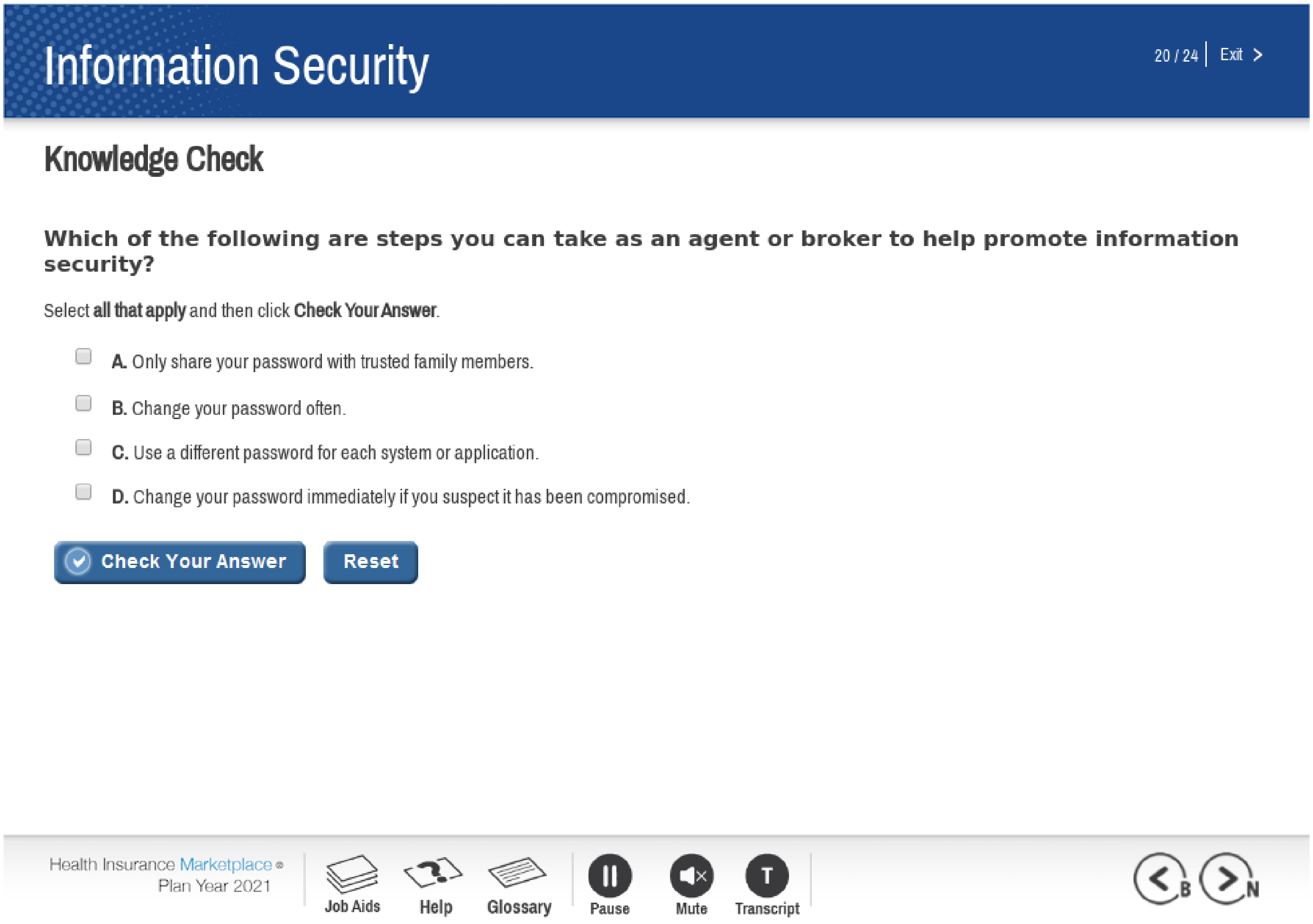
Positive Feedback

Correct! Security awareness training and restricting access to systems with sensitive information are examples of controls.

Negative Feedback

Incorrect. The correct answers are A and C. Security awareness training and restricting access to systems with sensitive information are examples of controls.

Page: 20 of 24: Knowledge Check



Information Security

20 / 24 | Exit >

Knowledge Check

Which of the following are steps you can take as an agent or broker to help promote information security?

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

□ **A.** Only share your password with trusted family members.

□ **B.** Change your password often.

□ **C.** Use a different password for each system or application.

□ **D.** Change your password immediately if you suspect it has been compromised.

Prompt

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

Question

Which of the following are steps you can take as an agent or broker to help promote information security?

Options

A. Only share your password with trusted family members.
B. Change your password often.
C. Use a different password for each system or application.
D. Change your password immediately if you suspect it has been compromised.

Correct Answer

B, C, D

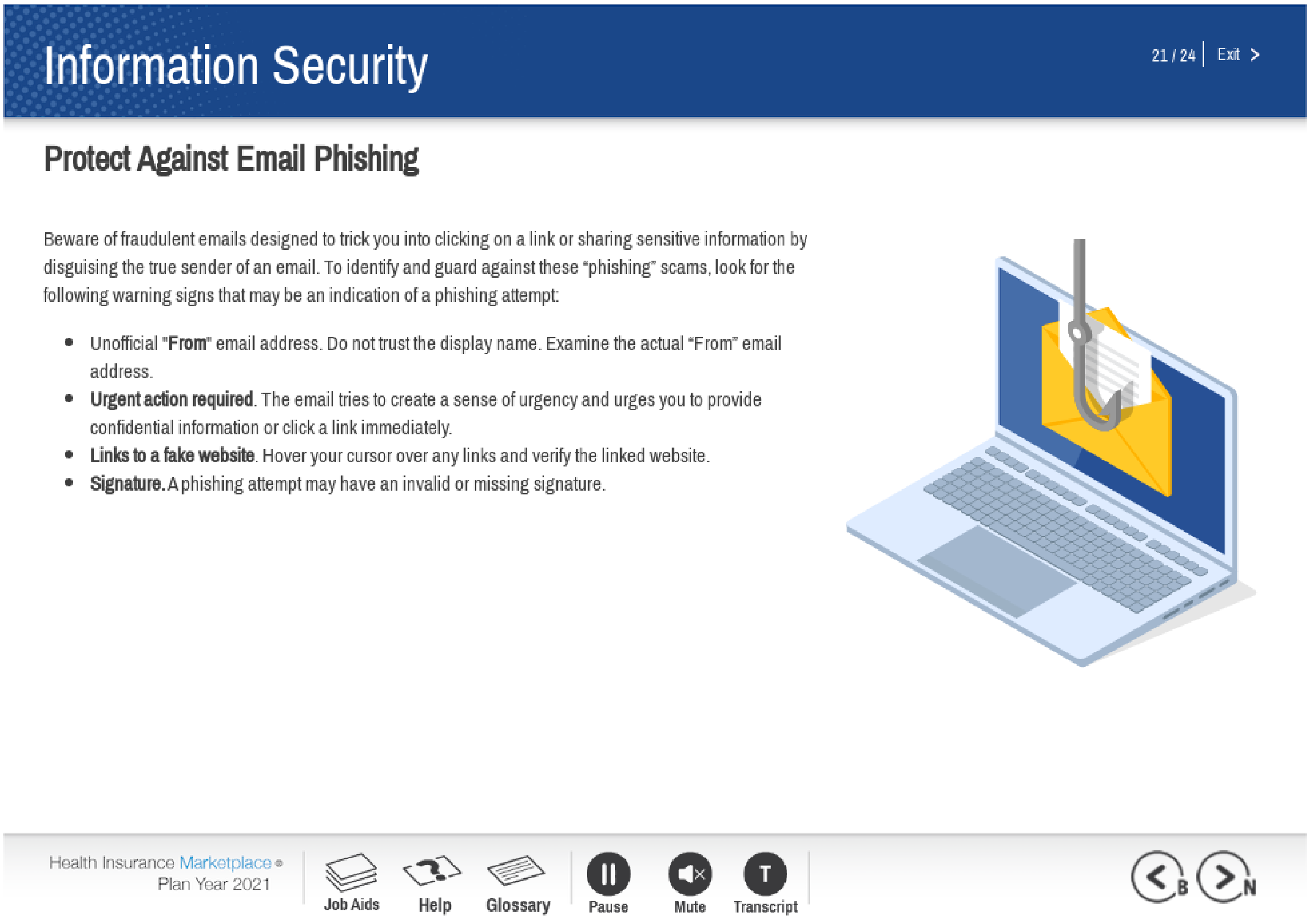
Positive Feedback

Correct! You should never share your password with anyone, even trusted family members.

Negative Feedback

Incorrect. The correct answers are B, C, and D. You should never share your password with anyone, even trusted family members.

Page: 21 of 24: Protect Against Email Phishing



Information Security

Protect Against Email Phishing

Beware of fraudulent emails designed to trick you into clicking on a link or sharing sensitive information by disguising the true sender of an email. To identify and guard against these “phishing” scams, look for the following warning signs that may be an indication of a phishing attempt:

- Unofficial "**From**" email address. Do not trust the display name. Examine the actual “From” email address.
- **Urgent action required**. The email tries to create a sense of urgency and urges you to provide confidential information or click a link immediately.
- **Links to a fake website**. Hover your cursor over any links and verify the linked website.
- **Signature.** A phishing attempt may have an invalid or missing signature.

Page Text

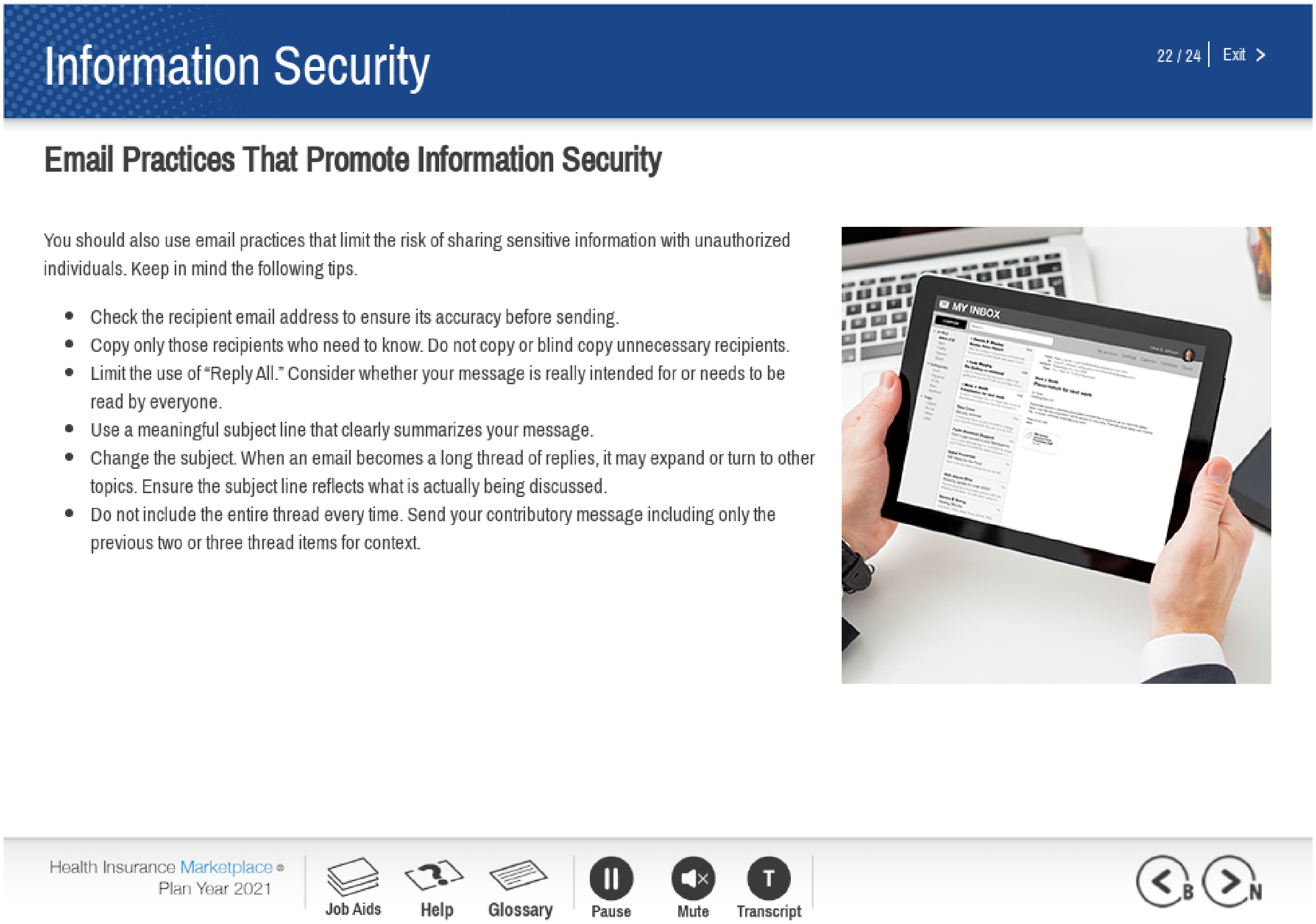
Beware of fraudulent emails designed to trick you into clicking on a link or sharing sensitive information by disguising the true sender of an email. To identify and guard against these “phishing” scams, look for the following warning signs that may be an indication of a phishing attempt:

- Unofficial "**From**" email address. Do not trust the display name. Examine the actual “From” email address.
- **Urgent action required.** The email tries to create a sense of urgency and urges you to provide confidential information or click a link immediately.
- **Links to a fake website.** Hover your cursor over any links and verify the linked website.
- **Signature.** A phishing attempt may have an invalid or missing signature.

Alt Text

A laptop with a yellow, open envelope displayed on the screen; a letter is coming out of the envelope; a fishing hook is trying to hook the letter

Page: 22 of 24: Email Practices That Promote Information Security



Email Practices That Promote Information Security

You should also use email practices that limit the risk of sharing sensitive information with unauthorized individuals. Keep in mind the following tips.

- Check the recipient email address to ensure its accuracy before sending.
- Copy only those recipients who need to know. Do not copy or blind copy unnecessary recipients.
- Limit the use of “Reply All.” Consider whether your message is really intended for or needs to be read by everyone.
- Use a meaningful subject line that clearly summarizes your message.
- Change the subject. When an email becomes a long thread of replies, it may expand or turn to other topics. Ensure the subject line reflects what is actually being discussed.
- Do not include the entire thread every time. Send your contributory message including only the previous two or three thread items for context.

Page Text

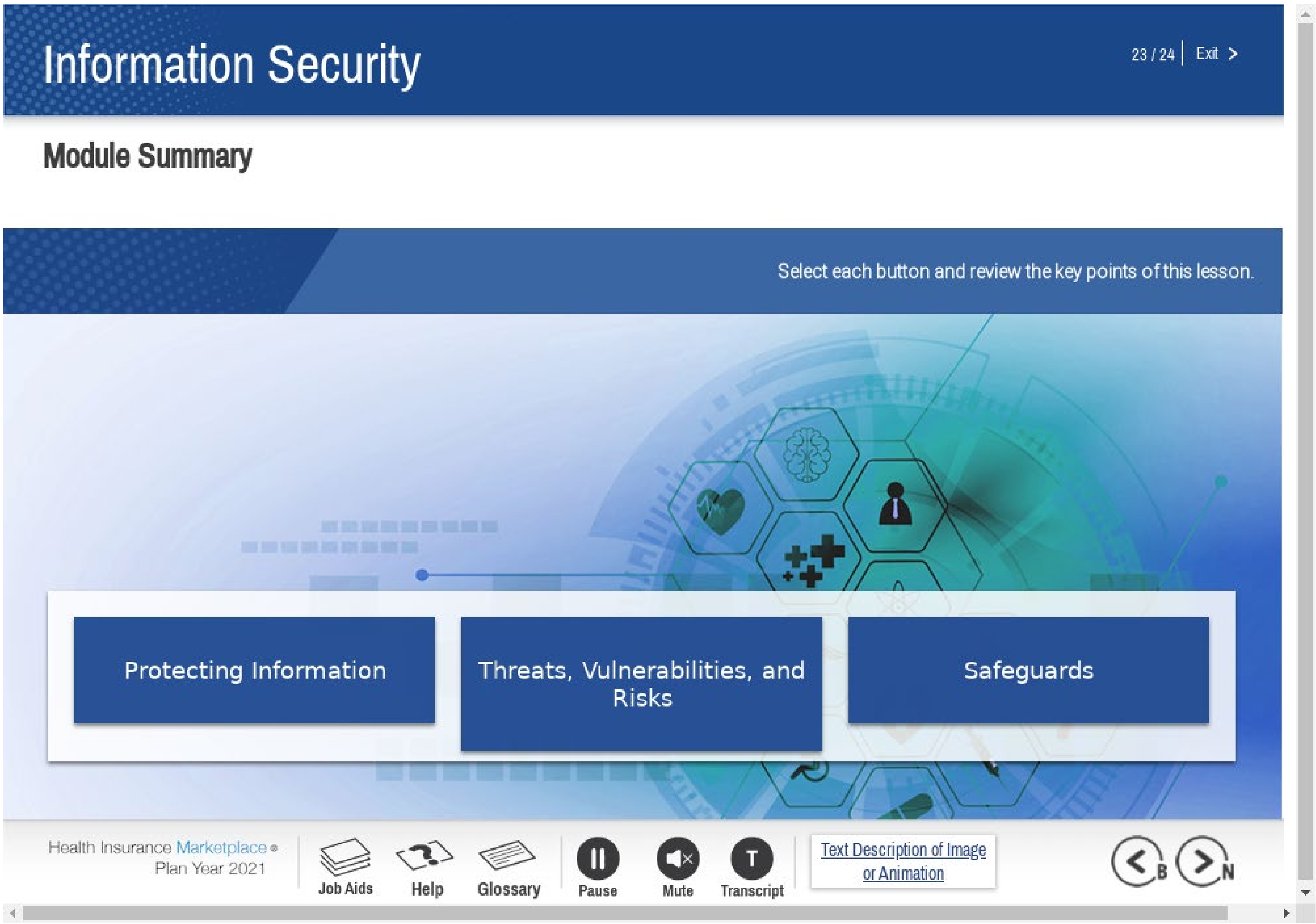
You should also use email practices that limit the risk of sharing sensitive information with unauthorized individuals. Keep in mind the following tips.

- Check the recipient email address to ensure its accuracy before sending.
- Copy only those recipients who need to know. Do not copy or blind copy unnecessary recipients.
- Limit the use of “Reply All.” Consider whether your message is really intended for or needs to be read by everyone.
- Use a meaningful subject line that clearly summarizes your message.
- Change the subject. When an email becomes a long thread of replies, it may expand or turn to other topics. Ensure the subject line reflects what is actually being discussed.
- Do not include the entire thread every time. Send your contributory message including only the previous two or three thread items for context.

Alt Text

A person holding a tablet displaying an email inbox

Page: 23 of 24: Module Summary



Information Security

23 / 24 | Exit >

Module Summary

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

Protecting Information
Threats, Vulnerabilities, and Risks
Safeguards
Health Insurance Marketplace
Plan Year 2021
Job Aids
Help
Glossary
Pause
Mute
Transcript
Text Description of Image or Animation
B
N

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. When each button is selected a popup box appears and displays accompanying text.

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

Protecting Information

Protecting Information Pop Up text:

- 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.

Threats, Vulnerabilities, and Risks

Threats, Vulnerabilities and Risks Pop Up text:

- There are three key elements to protecting information: confidentiality, availability, and integrity.
- A threat is the potential to cause unauthorized disclosure, changes to, or destruction of 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.

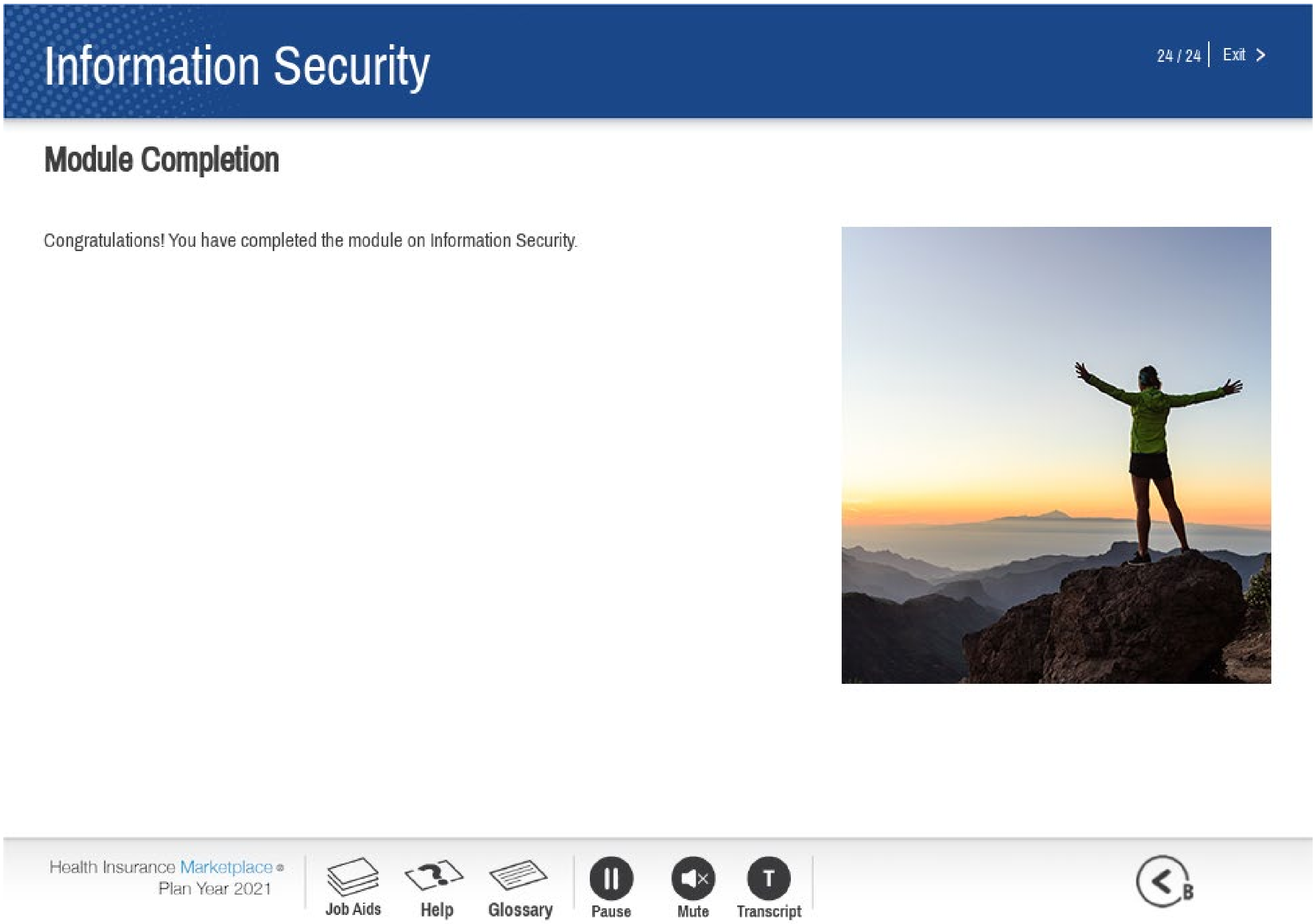
- A risk is the likelihood that a threat will exploit a vulnerability.

Safeguards

Safeguards Pop Up text:

- Agents and brokers can apply certain controls—policies, procedures, and practices that manage risk and protect IT assets—to protect consumer information.
- There are steps agents and brokers can take to help promote information security. Most importantly, NEVER share your passwords or login credentials, NEVER allow anyone (including clients) to share their private login credentials with you (including for HealthCare.gov), and only conduct person searches for consumers who have given you consent to assist them with applying for and enrolling in a Marketplace plan.

Page: 24 of 24: Module Completion



Information Security

24 / 24 | Exit >

Module Completion

Congratulations! You have completed the module on Information Security.

Page Text

Congratulations! You have completed the module on Information Security.

Alt Text

A person standing on a mountain peak with arms outstretched