This training provides the U.S. Department of Health and Human Services (HHS) employees, contractors, interns, and others with the knowledge to protect HHS information and information systems, and to minimize the risks of internal and external cyber threats. The goal of this training is to inform the HHS workforce of threats to HHS information and information systems, and provide best practices to defend the HHS mission from these threats.

Learner’s Corner

- The transcript icon on the upper right provides access to the transcript document.
- When necessary, the footnote text follows immediately the reference.
- Navigation to lessons is provided in the upper right section of the page or in the bookmarks.
- Click on the X in the top right corner of the window or ALT+F4 to close forms and pop-up windows.
- The training is fully accessible through keyboard and shortcuts.

This training fulfills the Federal Information Security Modernization Act of 2014 requirement and HHS IS2P recommendation for security awareness training for users of federal information systems.
What do hackers look for?

Hackers and adversaries are constantly seeking personally identifiable information (PII) and protected health information (PHI) stored on HHS information systems for the purpose of committing health insurance fraud, identity theft, and other financial crimes. As an HHS employee, contractor, intern, or Commissioned Corps of the U.S. Public Health Service personnel, you are a target because you have access to what the cybercriminals are looking for—PII, PHI, financial, personnel, grant, research, and patient medical information.

Hackers’ Methods to obtain your information

- Unattended devices
- Email/ Phone scams
- Compromised passwords

Information from your online profiles
TRAINING OBJECTIVES

Click on the objective icon below to the left or use the down arrow to advance to the next objective.

Objective 1

Develop and demonstrate foundational-level knowledge of cybersecurity.
Objective 1

Develop and demonstrate foundational-level knowledge of cybersecurity.

Objective 2

Employ best practices to protect privacy and safeguard Controlled Unclassified Information (CUI).
TRAINING OBJECTIVES

Click on the objective icon below to the left or use the down arrow to advance to the next objective.

Objective 1
Develop and demonstrate foundational-level knowledge of cybersecurity.

Objective 2
Employ best practices to protect privacy and safeguard Controlled Unclassified Information (CUI).

Objective 3
Recognize cyber threats to information systems.
TRAINING OBJECTIVES

Objective 1

Develop and demonstrate foundational-level knowledge of cybersecurity.

Objective 2

Employ best practices to protect privacy and safeguard Controlled Unclassified Information (CUI).

Objective 3

Recognize cyber threats to information systems.

Objective 4

Identify and report potential cybersecurity and privacy incidents promptly.
In this training, we will discuss why you need cybersecurity in the workplace, how to secure HHS information, and how to identify social engineering tricks often used by cyber criminals. We will also describe different types of cybersecurity breaches and how to report them.

<table>
<thead>
<tr>
<th>1</th>
<th>CONTROLLED UNCLASSIFIED INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Definitions and examples of CUI, PII and PHI.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>SECURING INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Best practices to protect HHS information assets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>SOCIAL ENGINEERING</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Methods used to manipulate people.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>BREACHES &amp; REPORTING</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>What are breaches and how to report them?</td>
</tr>
</tbody>
</table>
LESSON 1 — CUI

OVERVIEW
This lesson describes cybersecurity and the different types of Controlled Unclassified Information (CUI), including PII and PHI. The lesson also identifies best practices for you to apply within your workplace.

OBJECTIVES
• Define Cybersecurity.
• Describe the different types of CUI.
• Define and give examples of PII and PHI.

1 CONTROLLED UNCLASSIFIED INFORMATION
Definitions and examples of CUI, PII and PHI.
• What is Cybersecurity?
• What is CUI?
• Definitions and examples of PII and PHI.
Cybersecurity is the action taken to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

On a daily basis, we use many convenient ways to access information and information systems. They include the use of passwords, personal identity verification (PIV) cards, email, remote access, etc. Using the best practices within this training on a daily basis helps HHS personnel protect HHS information from hackers attempting to gain access.
### WHAT IS CUI?

**Controlled Unclassified Information**

CUI (sensitive data) is information that has a degree of confidentiality such that its loss, misuse, unauthorized access, or modification could compromise the element of confidentiality and thereby adversely affect national health interests, the operation of HHS programs, or the privacy of the Health Insurance Portability and Accountability Act (HIPAA).

In this training, we will refer to sensitive data as **CUI**.

<table>
<thead>
<tr>
<th>Types of CUI</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Personally Identifiable Information (PII)</td>
</tr>
<tr>
<td>• Protected Health Information (PHI)</td>
</tr>
<tr>
<td>• Intellectual Property</td>
</tr>
<tr>
<td>• Financial Data</td>
</tr>
</tbody>
</table>

In this training, we will focus on **PII and PHI**.

---

The CUI framework outlined in the NIST SP 800-60 Rev 1 memo is intended to replace common—but inconsistently applied—markings such as For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) with one framework for the federal government to designate, mark, safeguard, and disseminate information.
## What is PII?

PII is “information which can be used to distinguish or trace an individual's identity, such as their name, social security number (SSN), biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.”

1. Defined by OMB M-07-12.

## What is PHI?

PHI is defined as any individually identifiable health information that is explicitly linked to a particular individual and health information which can allow individual identification.

PHI also includes many common identifiers as name, address, birth date, and social security number.

Click on the PII/PHI icon for examples.

Read the following scenario, and then answer the question.

Please select from the answers below.

Do you think the following information can be used to identify Mr. Rabia?

A dentist office recently provided Ms. Jasmin Smith with a copy of her referral documents for the orthodontist. The following information was accidentally included in the file forwarded to Ms. Smith:

- **Applicant name:** Mr. Renee Rabia
- **Height:** 6”
- **Eye color:** Brown
- **Hair color:** Brown
- **Zip Code:** 22033
- **Birthplace:** Mozambique  **Age:** 40
- **City of Residence:** Fairfax, VA

Yes

No
In this lesson, you learned to:

• Define cybersecurity, CUI, PII and PHI.
• Identify CUI, PII and PHI.

Your ability to identify and protect CUI, including PII and PHI, will help you integrate a solid foundation of cybersecurity best practices into your daily work tasks, and projects.
LESSON 1 – QUIZ 1

Read the scenario below and answer the question. Please select from the answers below.

1) In 2016, a hospital reported to the Department a security breach that affected the records of up to 405,000 patients, employees, and employees’ beneficiaries. What type of data was lost?

A. PII  
B. PHI  
C. Both  
D. None
2) Jane works in a medical facility. Jane’s sister, Sharon, treated in the same facility, asked her to check her lab results. Can Jane give her sister the results?

A. Yes  
B. No
OVERVIEW
All HHS employees, contractors, and personnel have a responsibility to protect HHS information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

OBJECTIVES
• Identify the characteristics of a “strong” password.
• Apply GFE protection rules.
• Create and send encrypted email.
• List steps to store and dispose of data.

SECURING INFORMATION
Best practices to protect HHS information assets.

• PIV Card and Passwords.
• Wi-Fi Networks.
• GFE during Foreign Travel.
• Email Use and Encryption.
• Data storage and Disposal.
Personal Identity Verification Card

Personal Identity Verification (PIV) cards are official government-issued identification cards that permit you authorized access to HHS government buildings and secured areas based on your job role. You will also use it as an authentication device to access your government-issued computer. PIV cards contain your digital credentials used to encrypt emails, digitally sign documents, and verify physical access privileges.
**Lesson 2 Brain Teaser 1**

Time to tease your brain with a quick question!

*Do you want to learn more? Click on the Tip icon to the right for the best practices to protect your PIV card.*

You received an encrypted email and want to read it. Do you need your PIV card to decrypt the email message? Yes or No?

*Click on the question mark icon to see the answer.*
Strong Passwords

What are “Strong” Passwords? A strong password includes a random combination of 8 or more numbers, symbols, capital and lower-case letters. Using a variety of character types increases the time it takes to crack the password. Please use an easily remembered phrase and substitute letters and numbers for words. This is called a passphrase. Here’s an example: “I Like To Sing and Take Long Walks” = 1L2$&Tlw.

Click on the key image for strong password characteristics.

Do Not...

- Create easy-to-remember passwords.
- Use obvious passwords related to common information such as a child’s or pet’s name, or your favorite sports team.
- Use passwords that someone can guess, using your social media information.
- Write down your password in a place that is accessible to others.
- Share your password with anyone, including systems administrators.

1. For additional information, please see the HHS ISP policy on passwords at—OIS Policies, Standards, Memoranda & Guides.
Now that we’ve discussed the topic of passwords, let’s answer a question.

Do you want to learn more? Click on this Tip icon.

Which of the following is a good way to remember a password?

A. Use a favorite team name.
B. Use a familiar word with your birthdate.
C. Create a word with your child’s name.
D. Create a passphrase.
It’s important to remember that malicious actors could be lurking in the free Wi-Fi networks that you may be accustomed to accessing while at your local coffee shop, or while traveling. Do not expose your Government Furnished Equipment (GFE) to unnecessary security risks by connecting to free unsecure Wi-Fi networks. Only use secured Wi-Fi networks such as your home Wi-Fi or Hotspot devices (mobile phone/tablet).

*Click on the blue ball to the right for more guidelines.*
LESSON 2 KNOWLEDGE CHECK

Read the following scenario, and then answer the question.

Please select from the answers below.

You are a grant management analyst and you’re attending a workshop in a hotel conference center. It’s now during your lunch break and you receive a phone call from your supervisor asking you to email some important grant documents to her. You only have access to the conference center’s guest Wi-Fi, which is open for public use.

Ideally, which action is NOT recommended from the below list?

A. Apologize to your supervisor that you cannot send her the list until you are connected to a secure Wi-Fi.

B. Use a secure browser and secure VPN if you have one.

C. Send your supervisor the information using the unsecure Wi-Fi at the hotel.

D. Do not work on sensitive materials while connected to unsecure Wi-Fi.
According to the HHS Chief Information Officer, Use of Government Furnished Equipment (GFE) During Foreign Travel memo (dated December 2016), “HHS travelers should not have any expectation of privacy regarding any communication while traveling to foreign countries. Moreover, one may expose and compromise GFE to an increased level of risk during foreign travel. Someone other than the intended recipient may intercept unencrypted email communications and non-secure phone calls and our adversaries overseas and other bad actors, such as international criminal organizations, often target GFE. **HHS GFE is not permitted on unofficial, personal foreign travel.** All HHS personnel traveling abroad on official business must follow the Office of Security and Strategic Information’s (OSSI) Foreign Travel Checklist guidelines and contact OSSI at International@hhs.gov as early as possible."
**HHS Email Accounts**

HHS email accounts are for official government business; however, employees may have limited personal use of their HHS email. Employees should *NEVER conduct official HHS business* with their personal email accounts.\(^1\)

**Do Not…**

- Use your HHS email address to create personal commercial accounts for the purpose of receiving personal notifications, set up a personal business or website, or to sign up for memberships.
- Let your personal emails disrupt your productivity, interrupt service, or cause congestion on the network (e.g., sending spam or large media files), or to engage in inappropriate activities.

---

1. Review the Rules of Behavior for Use of HHS Information Resources for more information.
Encryption

*Encryption* is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not prevent interception, but denies the unauthorized persons and software the ability to interpret the message content. HHS policy requires files containing CUI to have encryption enabled while in transfer and while stored.¹ Emails that contain CUI must have encryption enabled before the sender sends them.

¹-Be sure to refer to your Operating Division Help Desk for instructions on how to use encryption technology. Encryption information and alternatives can be found by visiting HHS Cybersecurity Program Encryption.
When encrypting emails using Microsoft (MS) Outlook® and a PIV card, it’s important to remember that the email can only be unencrypted by internal HHS recipients. If the user is sending an encrypted email from an HHS email account to an external recipient, the recipient will not be able to unencrypt or read the content of the email. When the recipients open the email, they will enter their PIN number and MS Outlook® will decrypt and display the contents of the email.

Click on the red box in the right corner for an example of an encrypted message.

**Email Encryption Steps:**

1. Insert your PIV card into the PIV card reader.
2. Under the **Home** tab, select “New Email.”
3. Under the **Options** tab, select the “Encrypt”
4. Type your message and hit “**Send**” button.
Let’s see if you’ve learned what is needed to open an encrypted email.

Which of the following items are necessary when opening an encrypted email?
A. E-signature.
B. Digital certificate.
C. User’s PIN.
D. PIV Card.

*Click on the question mark icon to see the answer.*
Data Storage is maintaining or storing CUI. When safeguarding CUI, back up all stored or transmitted information, encrypt them, and file/archive the encrypted backup information.

Data Disposal: If a media device containing CUI is obsolete or no longer usable or required, it should be disposed in accordance with applicable laws and regulations. Disposal rules apply to information in paper, computer, or any other format.¹

Click on the folders icon on the right for data disposal methods.

¹ For more information, visit the Record Management webpage.
In this lesson, you learned how to:

• Create and protect strong passwords.
• Protect your PIV card from unauthorized use.
• Send an encrypted email.

Applying these best practices will help protect HHS information and information systems from hackers. Cybersecurity starts with you!
Read the scenario below and answer the question. Please select from the answers below.

Which of the following answers list the correct steps to send an encrypted email in MS Outlook® 2010?

**Choice A**
1. Insert your PIV card into the PIV card reader.
2. Under the Home tab, select “New Email.”
3. Under the Options tab, check the “Request a Read Receipt” box.
4. Type your message and hit “Send” button.

**Choice B**
1. Insert your PIV card into the PIV card reader.
2. Under the Home tab, select “New Email.”
3. Under the Options tab, select the “Encrypt” icon.
4. Type your message and hit the “Send” button.

**Choice C**
1. Insert your PIV card into the PIV card reader.
2. Under the Home tab, select “New Email.”
3. Under the Options tab, select the “Permission” icon.
4. Type your message and hit the “Send” button.

**Choice D**
1. Insert your PIV card into the PIV card reader.
2. Under the Home tab, select “New Email.”
3. Under the Options tab, check the “Request a Delivery Receipt” box.
4. Type your message and hit the “Send” button.
2) Mark is a new employee who just joined the Department. He received an email from the Help Desk to update his profile in the staff directory. The email included a link that Mark was instructed to click for access to his profile. The email also includes a telephone number for additional assistance.

What should Mark do?

A. Click on the link to update his profile.
B. Call the Help Desk number on the Intranet to verify the email.
C. Delete the email; it’s spam.
D. Mark should call the number given in the email to confirm the request.
OVERVIEW
Welcome to Lesson 3! In this lesson, we will identify how social engineers use phishing, phone scams, and social media to bait unsuspecting HHS employees into providing them access to HHS information and information systems.

OBJECTIVES
• Define social engineering and the types of attacks associated with it.
• Identify and report phishing emails.
• Determine ways to limit information posted on social media.
• Recognize techniques to handle suspicious phone calls.
• Identify and report Insider Threats.
It’s critical that you understand the most common methods used by criminals to manipulate people into providing information. Social engineering (human manipulation) is the use of deception to manipulate individuals into divulging confidential or personal information that the social engineer may use for fraudulent purposes. Malicious actors could appear to be a coworker or a “friend” in an effort to gain your trust so that they can obtain access to HHS information and information systems through you.
PHISHING

What’s Phishing?
Phishing is a social engineering scam whereby intruders seek access to information and information systems by posing as a real business or organization with legitimate reason to request information.

Phishing emails (or texts) quite often alert you to a problem with your account and ask you to click on a link and provide information to correct the problem.

Click on the Hacker’s icon to the right for a phishing example.

How it works?
These emails look real and often contain the organization’s logo and trademark. The uniform resource locator (URL) in the email can resemble the authentic URL web address, for example, “Amazons.com” with a very minor spelling error that one can overlook. Links included in phishing emails can download malicious programs onto your computer or mobile device and allow the attacker access to the device, connected devices, and the information stored on those devices.
If you are suspicious of an email:

• Forward the email to spam@hhs.gov and then delete it permanently from your Inbox and Trash folders.
• Do not click on the links provided in the email.
• Do not open any attachments in the email.
• Do not provide personal information or financial data.
Let’s take a look at the following phishing brain teaser!

Brian received a phone call at work. “Tech Support” called to verify information on his computer. Brian was instructed to provide network and password information over the phone. Brian obliged and provided the requested information. Did Brian take the correct action? Yes or No?

Click on the question mark icon to see the answer.
It’s critical that you understand the threats you may encounter when using your social media accounts. Malicious actors may often pretend to be a coworker, a “friend,” or to have a common social media interest in an effort to gain your trust so that they can obtain unauthorized access to HHS information and information systems. To the right, there are some recommendations to ensure your information security.

• Do not associate your employment at HHS with your social media accounts.
• A social engineer may aggregate and use multiple posts about your job with malicious intent.
• Be mindful of what you tweet, Instant Message (IM), or post online because once it’s on the Internet it’s on the Internet forever!
Many people think cybercriminals only use phishing and other unethical computer tactics to obtain sensitive information from unsuspecting victims. However, cybercriminals use phone scams too. A cybercriminal could claim to be from a trusted location at work and ask for PII from an HHS employee. The employee may receive an email from "technical support" in which they should call a certain number to ensure that their computer is working correctly, or complete the installation of software. Be aware of these tactics and do not fall prey to social engineers.

*Click on the red circle to the left for a phone scam story.*
Read the following scenario, and then answer the question.

Allison received an email from a coworker she does not know regarding the upcoming office Holiday party. Included in the email is an attachment listing the attendees and the food items they are bringing to the party. The coworker has requested that Allison immediately review the list and verify what she will bring to the party.

Based on the answers provided below, what should Allison do next?

A. Examine the email and check for red flags indicating that it may be a phish.
B. Call the coworker to verify the legitimacy of the email.
C. If the recipient cannot verify the email, forward it to spam@hhs.gov.
D. All of the above.
Insider threats are the most extreme type of social engineering. An insider threat is a malicious threat to an organization that comes from current or former employees or contractors within the organization, who have inside information concerning the organization's security practices, data, and computer systems. Instances of insider threats are rare but very serious.

HHS is a multi-disciplined, geographically distributed public health enterprise whose missions include research, innovation, regulation, prevention, and response. HHS has information of interest to foreign intelligence agents or organizations, and insider threats. If you have significant reason to suspect an employee is an insider threat, report it to the OSSI: Counter-intelligence Directorate at awareness@hhs.gov.
In this lesson, you learned how to:

• Report suspicious emails to spam@hhs.gov and verify links and file attachments before clicking on them;

• Be aware of human manipulation methods used by cybercriminals to trick you into providing Controlled Unclassified Information (CUI); and

• Report suspicious activity to the OSSI: Counter-intelligence Directorate at awareness@hhs.gov

It’s important for you to identify these methods so that you can help prevent cybersecurity breaches.
Read the scenario below and answer the question. Please select from the answers below.

1) Updating his social media accounts is one of Trevor’s favorite activities. Trevor likes to tell everyone how lucky he is to work at HHS. One day, Trevor’s old friend Mike from high school sent him a “friend” request. Trevor hasn’t spoken to Mike in a while but accepted the friendship in hopes that they could catch up. Trevor clicks on a link in a social media instant message from Mike while working on his HHS laptop. The link went to a blank page. Trevor realized that the friend request was actually from someone he didn’t know. Trevor immediately “un-friended” the person.

Should Trevor worry about his HHS laptop being compromised?

A. Yes  
B. No
Read the scenario below and answer the question. Please select from the answers below.

2) Lucy sent her coworker an email containing CUI just before the end of her workday. The next day, Lucy realized she forgot to encrypt the email.

Should Lucy be concerned?

A. Yes
B. No
OVERVIEW

Welcome to Lesson 4! In this lesson, we will learn how to prevent and limit the impact of a breach by identifying incidents and learning when and how to promptly report them.

OBJECTIVES

• Identify the different types of cybersecurity and privacy incidents.
• Examine information and differentiate public from private use.
• Perform the steps to report a suspected or confirmed cybersecurity or privacy incident to proper authorities.

4 BREACHES AND REPORTING

What are breaches and how to report them?

• Recognize Incidents
• Reporting Incidents
**RECOGNIZING INCIDENTS**

**Information Security Incidents**

Understanding the actions and situations that can cause a security incident is critical to the protection of HHS information and information systems. To the right is a list of incidents that must be reported immediately to the 24-hour Computer Security Incident Response Center (CSIRC) at csirc@hhs.gov and to your OpDiv’s Incident Response Team.

<table>
<thead>
<tr>
<th>Types of Incidents:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Loss, damage, or theft, of equipment, media, or documents containing PII.</td>
</tr>
<tr>
<td>• Accidentally sending a report containing PII to a person not authorized to view the report or sending it unencrypted.</td>
</tr>
<tr>
<td>• Allowing an unauthorized person to use your computer or credentials to access PII.</td>
</tr>
<tr>
<td>• Discussing CUI in a public area.</td>
</tr>
<tr>
<td>• Accessing the private records of friends, neighbors, celebrities, etc. for casual viewing.</td>
</tr>
<tr>
<td>• Any security situation that could compromise HHS information or information systems (e.g., virus, phishing email, social engineering attack).</td>
</tr>
</tbody>
</table>
Time for a question!

One day, Katherine realized that she forgot to bring her laptop to work. She needed to finalize a presentation for her meeting at 1PM. Katherine’s coworker, Dan, agreed to let her use his computer once he completed his monthly report. After Dan finished his report, he gave his laptop to Katherine with his PIV card still inside. Katherine completed her presentation, but before giving Dan his computer back, she decided to take a look at a few shared folders that she realized she didn’t have access to on her own laptop. Katherine then returned the laptop and thanked Dan for his help. Should Dan consider this an “incident?”
REPORTING INCIDENTS

It’s important to understand what an “incident” is, and how to report one should one occur. Reporting all possible security incidents immediately gives the 24-hour CSIRC and your OpDiv’s Incident Response Team the best chance to minimize the negative impact of the incident. Today’s high-speed internet connections can allow an adversary to steal gigabytes of data in minutes. Every second counts when it comes to reporting security incidents. Failing to report an incident immediately allows the hacker to operate unnoticed in the HHS network for a longer period of time. Ethically, it is your responsibility to report incidents as soon as you identify them. So stay alert! Your quick response can prevent a breach.

The scenarios in this lesson will help you understand how to quickly take action when incidents happen. If any privacy or data incidents occur (as listed in the “Recognizing Incidents” section), please report them at once! Click on the image to the right for the list of HHS OpDiv Incident Response Teams.
Read the following scenario, and then answer the question.

Please select from the answers below.

Tammy and Jill went to a local coffee shop for a short break. Over coffee, they discussed client details and other CUI relating to their department. At the end of their discussion, they realized that someone from another department had been watching them and listening to their discussion a few tables away. This person should not have heard any of their private discussion. What should they do?

A. Ignore the eavesdropper...maybe this person didn’t hear the discussion after all.

B. Ask the eavesdropper not to disclose any information that s/he overheard.

C. Immediately report the “incident” to the 24-hour CSIRC (csirc@hhs.gov) and to your OpDiv’s Incident Response Team.

D. None of the above.
In this lesson, you learned how to:

- Define and identify types of cybersecurity incidents.
- Report an incident.

Being able to identify and report an “incident” is imperative in a workplace that deals with highly sensitive information. The impact of some incidents can be minimized by simply encrypting emails containing CUI, and/or by your quick action to report an incident. These are all simple actions, yet imperative and mandated. Remember, report all breaches to the 24-hour CSIRC (csirc@hhs.gov) and to your OpDiv’s Incident Response Team. Report malicious/spam emails to spam@hhs.gov.
LESSON 4 - QUIZ 1

Read the scenario below and answer the question. Please select from the answers below.

1) Carol realized that she forwarded a sensitive HHS email to the wrong person.

What should she do?

| A. Immediately report the “incident” to the 24-hour CSIRC (csirc@hhs.gov) and to your OpDiv’s Incident Response Team. |
| B. Inform the recipient to disregard and delete the contents of the email that was sent erroneously. |
| C. Both. |
| D. None of the above. |
LESSON 4 - QUIZ 2

Read the scenario below and answer the question. Please select from the answers below.

2) An OpDiv experienced laptop thefts. What should the manager on site do?

A. Immediately report the “incident” to spam@hhs.gov.

B. No rush...but report the “incident” at some point this week.

C. Immediately report the “incident” to the 24-hour CSIRC (csirc@hhs.gov) and to your OpDiv’s Incident Response Team.

D. None of the above.
Understanding how to protect HHS CUI, PII, and PHI is critical to ensuring the mission of HHS. Training you to effectively apply cybersecurity best practices is the focus of this training. Identifying cybersecurity incidents and understanding how to report them will improve the security posture of HHS information and information systems. You are encouraged to immediately apply the best practices you learned from this training into your daily work habits.

In this training, you learned to:

- Define cybersecurity and Controlled Unclassified Information (CUI).
- Define privacy and PII and means to protect PII in different contexts and formats.
- Create strong passwords and protect your PIV card from unauthorized use.
- Safeguard GFE during foreign travel.
- Define encryption and determine how and when to encrypt.
- Describe human manipulation methods often used by hackers.
- Report suspicious emails and activities to reporting authorities.
- Identify the different types of incidents including insider threats, and how to report them.
1) While at dinner with friends, a thief broke into Fred’s car and stole Fred’s HHS laptop. Fred is an HHS contractor. His laptop contained pictures of his children; five HHS grantee applications with grantees full names, home addresses, work addresses, SSN’s, employer identification numbers (EIN), and a couple of case files containing patient full name, address, gender, date of birth, medical record number, medical notes, address, and health care facility name.

Does Fred’s laptop contain PII?

A. Yes  B. No
Read the scenario below and answer the question. Please select from the answers below.

2) While at dinner with friends, a thief broke into Fred’s car and stole Fred’s HHS laptop. Fred is an HHS contractor. His laptop contained pictures of his children; five HHS grantee applications with grantees full names, home addresses, work addresses, SSN’s, employer identification numbers (EIN), and a couple of case files containing patient full name, address, gender, date of birth, medical record number, medical notes, address, and health care facility name.

In the previous scenario, which of the following is not HHS PII?

A. Grantee’s social security number
B. Patient’s date of birth
C. Pictures of Fred’s children
D. Patient’s gender
3) While at dinner with friends, a thief broke into Fred’s car and stole Fred’s HHS laptop. Fred is an HHS contractor. His laptop contained pictures of his children; five HHS grantee applications with grantees full names, home addresses, work addresses, SSN’s, employer identification numbers (EIN), and a couple of case files containing patient full name, address, gender, date of birth, medical record number, medical notes, address, and health care facility name.

Should Fred report this incident? Why or why not?

A. Yes, Fred should report the incident because he lost personal information.

B. Yes, Fred does need to report this incident because it involved HHS information. All HHS employees, contractors, and personnel are responsible for reporting cybersecurity breaches.

C. No, Fred does not need to report the incident because the computer is replaceable.

D. No, Fred should not report the incident because he is a contractor.
4) Alan works on the third floor at a medical clinic. Alan’s coworker, Debby, cannot get into the electronic health record (EHR) system, because she has failed to enter the correct password. In order to reset the password, Debby would have to go see a representative from the Password Distribution Center (PDC), on the first floor of the building, leaving the secured floor where she is located. Debby is unable to go to the PDC, because she cannot find her PIV card and believes she has misplaced it. Debby asks Alan for his login credentials, so that she may access the EHR system.

Should Alan allow Debby to use his credentials?

A. Yes, she is Alan’s trusted coworker.
B. Yes, if Alan’s manager gives him permission.
C. No, sharing user credentials is a privacy violation.
D. A and B
5) Alan decides not to share his credentials with Debby. Debby now asks to borrow Alan’s PIV card, so that she may leave the secured floor, and get her password reset at the PDC.

What should Alan do?

A. Give Debby his PIV so she can leave the floor to reset her password.
B. Alan should tell her to ask another coworker for their PIV card.
C. Alan should escort Debby to the PDC so she can get her password reset since she doesn’t have her PIV card.
D. B and C
Read the scenario below and answer the question. Please select from the answers below.

6) This time Alan decides not to let Debby borrow his PIV card, because it would create a privacy incident.

What other privacy incident has already occurred?

A. Debby asked to borrow Alan’s credentials.

B. Debby has misplaced her PIV card and cannot find it.

C. Debby asked to borrow Alan’s PIV card.

D. A and C
RESOURCES

Training Resources
Learn more about the Federal and Departmental laws and regulations that guide your cyber activities.

Additional Guidance
Additional resources and full URLs for useful links relating to information security are provided in the links below.

Acknowledge & Complete
Click the below link to learn how to complete the training and receive the Certificate of Completion.

HHS CATE Resources: The HHS Cybersecurity Awareness Training and Education (CATE) team has also developed CyberCare and Healthy Technology as additional resources for you. We hope that you find them helpful. At the end of the training, you will be asked to provide feedback relating to CyberCare.
Thank you for completing
The Cybersecurity Awareness Training