LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS CMS

ISPG-INFORMATION SECURITY and PRIVACY GROUP

OFFICE OF THE CHIEF INFORMATION OFFICER

The Centers for Medicare & Medicaid Services Information Systems Security & Privacy Awareness Training

Information Systems Security & Privacy Awareness Training

Information Systems Security and Privacy Awareness

- Introduction
- Information Security Overview
- Information Security Policy and Governance
- Physical Access Controls
- Email and Internet Security
- Security Outside of the Office
- Privacy
- Incident Reporting
- Summary
- Appendix
- HHS Rules of Behavior

Introduction
Information Systems Security and Privacy

This course is designed to provide the Centers for Medicare and Medicaid Services (CMS) employees, contractors, and others with access to CMS data, systems, and networks with knowledge to protect information systems and sensitive data from internal and external threats.

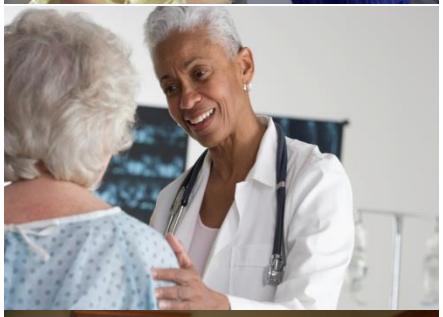
This course fulfills the Federal Information Security Management Act of 2002 (FISMA) requirement for security and privacy awareness training for users of Federal information systems.

The course will take approximately 60 minutes to complete.

At the end of the training, you will read and acknowledge the *HHS Rules of Behavior* at the end of the course.

The CMS Mission and You

CMS employees and contractors routinely access sensitive data like names, Social Security numbers, and health records to successfully carry out CMS' mission of protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves.



Introduction
CMS Data Users Are the Best Line of Defense

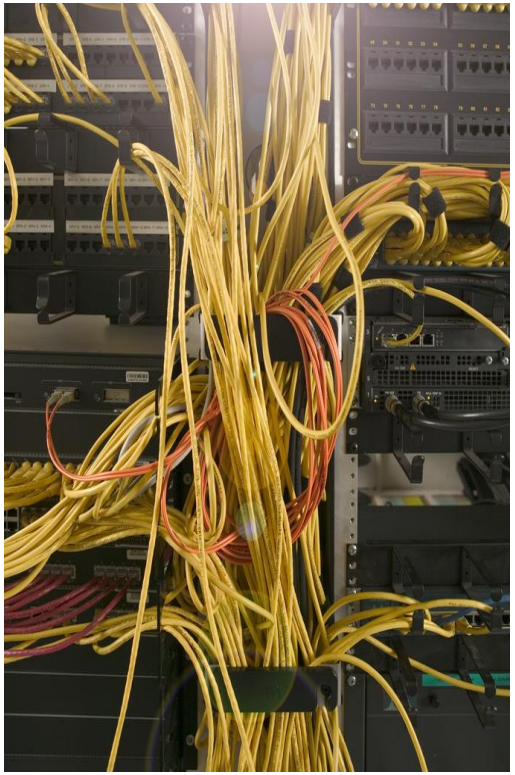
CMS personnel are critical to the defense and protection of sensitive Department information systems and data.

You will be well equipped to protect CMS by incorporating the information technology (IT) security and privacy objectives learned in this course into your daily work.

Introduction
Objectives

- At the end of the course, you will be able to:
- Define information systems security;
- Identify federal regulations that mandate the protection of IT assets;
- Understand CMS' IT security and privacy policy, procedures, and practices;
- Understand personal responsibility to protect information systems;
- Recognize threats to information systems and privacy;
- Identify best practices to secure IT assets and data in and out of the office;
- Define privacy and personally identifiable information (PII); and
- Identify the correct way to respond to a suspected or confirmed security or privacy incident.

Information Security Overview



Information Security Overview
Did You Know?

- The Office of Management and Budget (OMB) reported 43,889 separate cyber attacks on Federal networks in 2011; a 5% increase over 2010.

Source: "OMB: Growth In Federal Cyber Attacks Slows". National Journal. March 15, 2012

- The Internet Crime Complaint Center (IC3) reported that consumers lost $485 million due to Internet scams in 2011.

Source: Internet Crime Complaint Center, http://www.ic3.gov/media/2012/120511.aspx

- The Federal Trade Commission (FTC) counted 250,854 complaints about identity theft in 2010, meaning the crime accounted for 19% of the 1.3 million total complaints the agency received. Identity theft is at the top of the consumer complaint list for the 11th year in a row.

Source: Federal Trade Commission, http://www.ic3.gov/media/2012/120511.aspx

Every year cyber attacks become more sophisticated and result in large losses of personal and financial data. Knowledge about how to protect information systems is vital to the effectiveness of the CMS' operations and ability to accomplish our mission.

Information Security Overview
What is Information Security?

✓ **Objective**

Define information systems security

Information Security (IS) – 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 IS 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 HHS has a media neutral policy towards information, meaning that any data whether in electronic, paper, or oral format must be protected.

Information Security Overview

Key Concepts

There are three elements to protecting information:

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

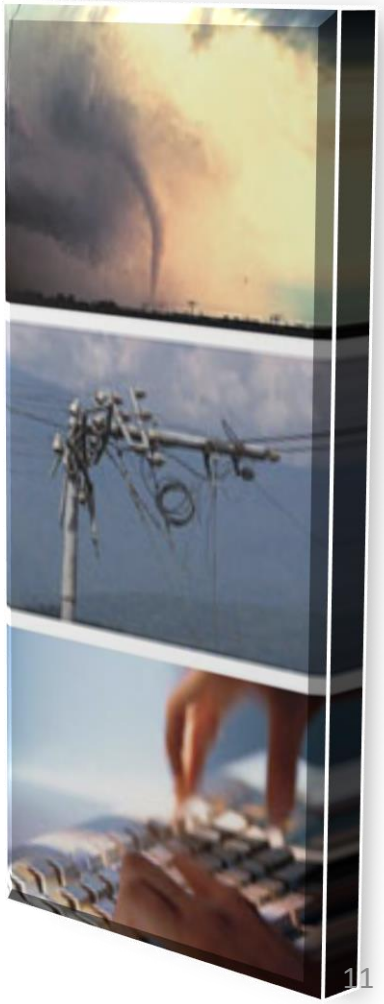
Your bank ATM is a good example of an information system that must be confidential, available, and have integrity.

- Imagine if your account was not kept **confidential** and someone else was able to access it when they approached the ATM. How much damage could be done?
- Imagine if every time you went to the ATM, the balance it displayed was inaccurate. How could the poor **integrity** of your balance information adversely affect your account management?
- Imagine if your bank's ATM was rarely **available** when you needed it. Would you continue to use that bank?

Information Security Overview
Key Concepts

Threats and vulnerabilities put information assets at risk.

- **Threats** – the potential to cause unauthorized disclosure, changes, or destruction to an asset.
  - Impact: potential breach in confidentiality, integrity failure and unavailability of information
  - Types: natural, environmental, and man-made
- **Vulnerabilities** – any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy.
- **Risk** – the likelihood that a threat will exploit a vulnerability. For example, a system may not have a backup power source; hence, it is vulnerable to a threat, such as a thunderstorm, which creates a risk.



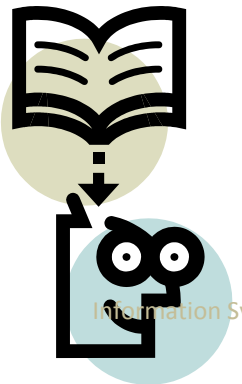
Information Security Overview
Key Concepts

- **Controls** – 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; and
  - Restricting access to systems that contain sensitive information.

Information Security Overview Knowledge Check

What is the goal of information security? *(choose the best answer)*

- A: Ensure that employee passwords contain at least eight characters including 1 number and 1 letter.
- B: Protect the confidentiality, integrity and availability of information and information systems.
- C: Eliminate all threats to information systems.
- D: Provide a lock for all file cabinets in the building.



Information Security Overview
Knowledge Check - Answer

The correct answer is:

The goal of information security is to protect the confidentiality, integrity, and availability of information and information systems.

Information Security Policy and Governance

Information Security Policy and Governance
Federal Government Governance

✓ **Objective:** Identify federal regulations that mandate the protection of IT assets

The table lists some sources of legislation and guidance that provide the backbone to governance that protects federal information and systems.

IT Security and Privacy Legislation and Guidance	National Institute of Standards and Technology (NIST) Special Publications
▸ E-Government Act of 2002 ▸ Clinger-Cohen Act of 1996 ▸ Health Insurance Portability and Accountability Act of 1996 (HIPAA) ▸ Office of Management and Budget (OMB) Circular A-130 ▸ Privacy Act of 1974 ▸ Paperwork Reduction Act ▸ Children's Online Privacy Protection Act (COPPA)	▸ NIST issues standards and guidelines to assist federal agencies in implementing security and privacy regulations. ▸ Special publications can be found at: http://www.nist.gov/publication-portal.cfm

Information Security Policy and Governance
Department Governance

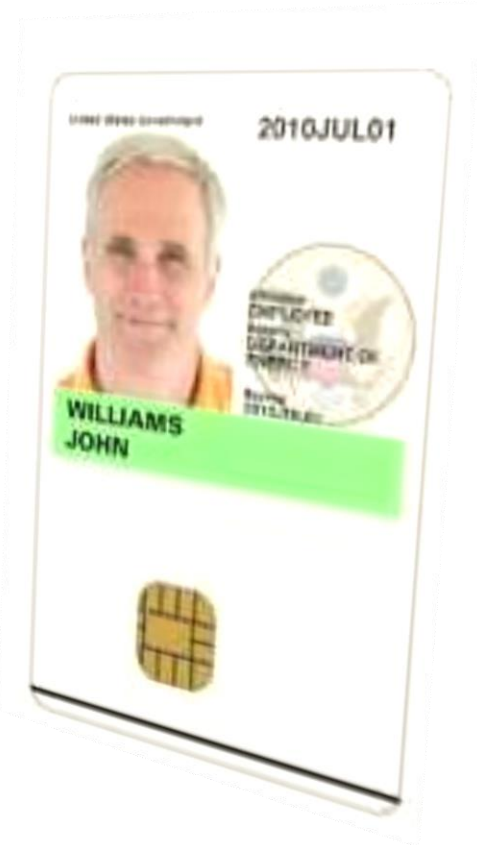
- The **Department** sets programmatic direction by providing an enterprise-wide perspective, facilitating coordination among key stakeholders, setting standards and providing guidance, and supporting streamlined reporting and metrics capabilities.
- **CMS Cybersecurity Program** is our information security program. Oversight is provided by the Office of the Chief Information Officer (CIO) and Chief Information Security Officer (CISO).
- **CMS** implements programs that meet specific business needs, provide business/domain expertise, manage implementation at the OpDiv level, develop policies and procedures specific to the operating environment, and manage ongoing operations.

Information Security Policy and Governance: Department Governance

✓ **Objective:** Understand CMS IT security policy, procedures, and practices

- The *HHS-OCIO Policy for Information Systems Security and Privacy* provides direction on developing, managing, and operating CMS IT security program.
- *HHS Rules of Behavior (For Use of HHS Information Technology Resources)* sets the policies for using Department systems. Operating Divisions may have additional policies and programs specific to their operating environment, however they shall not be less strict than the Department's rules.

Physical Access Controls



Physical Access Controls
Password Protection

✓ **Objective:** Identify best practices to secure IT assets and data in and out of the office

- A strong password for your network account and other applications is a basic protection mechanism.
- While it is tempting to create an easy or generic password that is easy to remember, it is not very secure.
  - **Two rules for stronger passwords:**
    - Create a password of least eight characters in length.
    - **Password should contain at least one each:**
      - Capital letter
      - Lowercase letter
      - Number

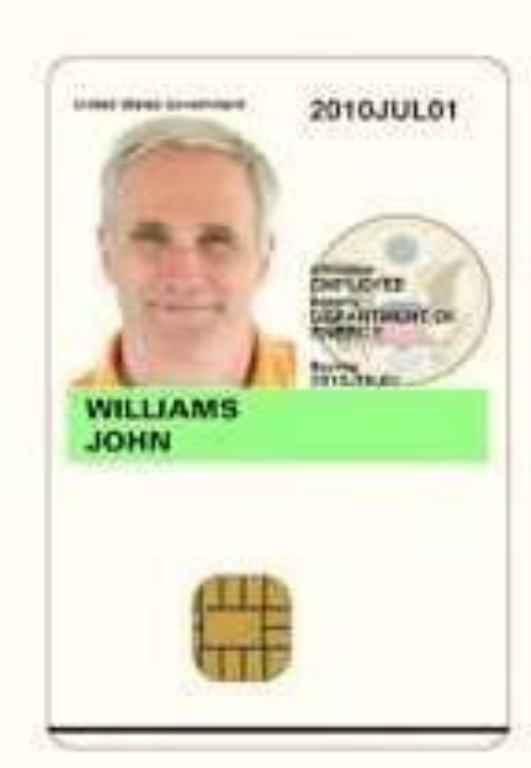
Physical Access Controls
Password Protection

- Having trouble remembering passwords? Use a passphrase.
  - Use the initials of a song or phrase to create a unique password
  - Example: “Take me out to the ballgames” becomes “Tmo2tBGs”
- Commit passwords to memory. If you are having trouble, then write it down and keep it in a secure place.
- **DO NOT** keep passwords near your computer or desk.

Physical Access Controls
Password Protection Tips

- Change password often. CMS will remind you to do this but if not, set up a reminder in your calendar at least every 60 days.
- Contact the CMS IT Service Desk if you suspect your password has been compromised.
- Create a different password for each system or application if applicable.
- Do not reuse passwords until six other passwords have been used.
- Do not use generic information that can be easily obtained like family member names, pet names, birth dates, phone numbers, vehicle information, etc.
- **NEVER** share your password with anyone.

Personal Identity Verification (PIV) Card



- PIV cards use radio frequency identification chips to reliably identify employees and contractors, and grant access to CMS buildings and government-issued computers.
- PIV cards contain PII about you and must be protected like a password.
  - Maintain possession of your PIV card at all times. Remember to remove it from your computer when you leave your workstation.
  - If your PIV card is lost or misplaced, report it to the security office immediately.
  - Keep your PIV card in a secure badge holder to shield it against unauthorized reading.

Physical Access Controls
Tailgating

- Physical security is an important information systems safeguard. Limiting access to information systems and infrastructure to authorized personnel diminishes the likelihood that information will be stolen or misused.

Combat tailgating

- Never allow anyone to follow you into the building or secure area without his or her badge.
- Be aware of procedures for entering a secure area, securing your workstation when you leave the office, and securing your workstation during emergencies.
- Do not be afraid to challenge or report anyone who does not display a PIV card or visitor's badge.
- Escort visitors to and from your office and around the facility.
- Do not allow anyone else to use your PIV card for building or secure area access.
- Report any suspicious activity to the security office.

Physical Access Controls
Physical Security Protection Tips

- Lock your computer when it is not in use.
- Remove your PIV card when leaving your workstation. Do not leave it in the card reader.
- Store and transport removable media such as CDs, DVDs, flash drives, and external hard drives in a secure manner to prevent theft or loss.
- Only connect government authorized removable media devices.
- Encrypt all devices which contain PII and sensitive information.
- Keep sensitive information out of sight when visitors are present.
- Quickly retrieve faxes that are sent to you. Always confirm that the recipient received the fax that you sent.

Physical Access Controls Knowledge Check

Which password is most secure?

- A: linda12
- B: 123Abc
- C: Big_Apples
- D: BH17Plus

Physical Access Controls Knowledge Check - Answer

The correct answer is:

BH17Plus is the most secure password because it contains:

- Upper case letters,
- Lower case letters,
- Numbers

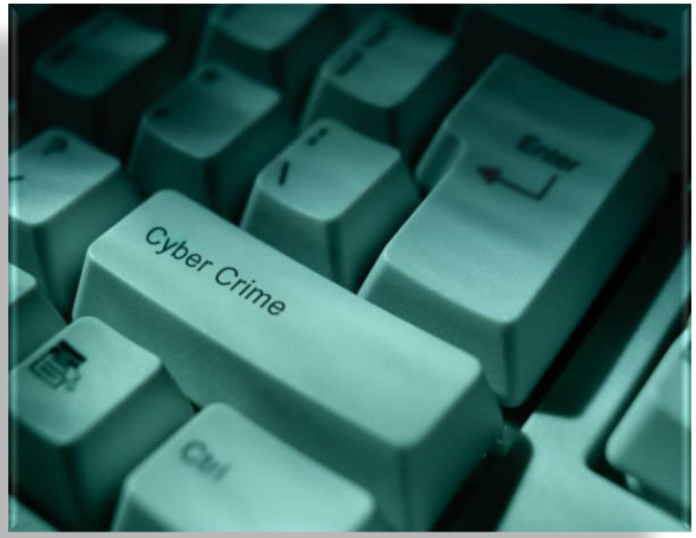
Email and Internet Security

Email and Internet Security
Cyber Crime

✓ **Objective:** Recognize threats to information systems and privacy

Cyber crime refers to any crime that involves a computer and a network. Offenses are primarily committed through the Internet.

- Common examples of cyber crime include:
  - Credit card fraud;
  - Spam; and
  - Identity theft.
- Government information and information system assets are a high value target.
- Criminals, terrorists, and nation states with malicious intent work daily to steal, disrupt, and change information systems at government agencies, including CMS.



Email and Internet Security
Social Engineering

- Social engineering is classically defined as the art of manipulating and exploiting human behavior to gain unauthorized access to systems and information for fraudulent or criminal purposes.
- Social engineering attacks are more common and more successful than computer hacking attacks against the network.

Email and Internet Security
Human Behavior

✓ **Objective:** Recognize threats to information systems and privacy

Social engineering attacks are based on natural human desires like:

- Trust
- Desire to help
- Desire to avoid conflict
- Fear
- Curiosity
- Ignorance and carelessness

Social engineers will gain information by exploiting the desire of humans to trust and help each other.

Email and Internet Security Targets

Social engineers want any information that will give them access to government systems or facilities. Common targets are:

- Passwords
- Security badges
- Access to secure areas of the building
- Uniforms
- Smart phones
- Wallets
- Employee's personal information

Email and Internet Security
Phishing Attacks

- Phishing is a social engineering scam whereby intruders seek access to your personal information or passwords by posing as a legitimate business or organization with legitimate reason to request information.
- Usually an email (or text) alerts you to a problem with your account and asks you to click on a link and provide information to correct the situation.
- These emails look real and often contain the organization's logo and trademark. The URL in the email resembles the legitimate web address. For example "Amazons.com".

Spear phishing is an attack that targets a specific individual or business. The email is addressed to you and appears to be sent from an organization you know and trust, like a government agency or a professional association.

Whaling is a phishing or spear phishing attack aimed at a senior official in the organization.

Email and Internet Security
Phishing Examples

Phishing emails appear to be legitimate. Take a look at these real-life examples:

- **Better Business Bureau complaint:** Executives receive an email that looks like it comes from the Better Business Bureau. The message either details a complaint a customer has supposedly filed or claims the company has been accused of identity theft. The recipient is asked to click a link to contest the claim. Once the link is clicked, a computer virus is downloaded.
- **Travel trouble:** An email appears to be a notice from an airline that you have purchased a ticket and arranged to check several bags. Many consumers, outraged because they never planned any such trip, click a link in the email to complain. The problem is, this clicking leads to an identity-theft page, where victims are asked to share sensitive data. If you receive such an email, simply ignore it.

Email and Internet Security
Combat Phishing

- **NEVER** provide your password to anyone via email.
- Be suspicious of any email that:
  - Requests personal information.
  - Contains spelling and grammatical errors.
  - Asks you to click on a link.
  - Is unexpected or from a company or organization with v do not have a relationship.
- If you are suspicious of an email:
  - **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.
  - **Do** forward the email to the HHS Computer Security Incident Response Center (CSIRC) or spam@hhs.gov and then delete it from your Inbox.

Email and Internet Security
Identity Theft

- The Federal Trade Commission estimates that 9 million people have their identity stolen each year.
- Identity thieves use names, addresses, Social Security numbers, and financial information of their victims to obtain credit cards, loans, and bank accounts for themselves.

If you believe you are a victim of identity theft:

- Contact the three credit reporting companies (Equifax, Experian, and Trans Union) and place a fraud alert on your report.
- Inform your bank, credit card issuers and other financial institutions that you are a victim of identity theft.
- If you know who stole your information, contact the police and file a report.

Email and Internet Security
Preventing Identity Theft

Combat identity theft

- Be cautious when providing your Social Security number. Know how and why it will be used.
- Review credit card and bank statements at least monthly for unauthorized transactions.
- Use strong passwords for your home computer and web sites you visit, especially email accounts and financial institutions.
- Leave your Social Security card and passport at home. Never leave them in your purse or wallet unless necessary.
- Shred sensitive documents and mail containing your name and address.

Email and Internet Security
Malware

Malware (short for malicious software) does damage to, steals information from, or disrupts a computer system.

- Malware is commonly installed through email attachments, downloading infected files, or visiting an infected web site.
- It can corrupt files, erase your hard drive, or give a hacker access to your computer.
- **Combat malware**
- Read email in plain text and do not use the preview pane.
- Scan attachments with antivirus software before downloading. Do not trust any attachments, even those that come from recognized senders.
- Delete suspicious emails without opening them.
- If you believe your computer is infected, contact the help desk or security POC.

Email and Internet Security
Internet Hoaxes

- Email messages that promise a free gift certificate to your favorite restaurant, plead for financial help for a sick child, or warn of a new computer virus are typically hoaxes designed for you to forward them to everyone you know.
- Mass distribution of email messages floods computer networks with traffic slowing them down. This is a type of distributed denial-of-service (DDoS) attack.

Combat Internet Hoaxes

- Do not forward chain letters, email spam, inappropriate messages, or unapproved newsletters and broadcast messages. This is a violation of the HHS-OCIO Policy for Personal Use of Information Technology Resources.
- Do not open emails from senders whom you do not recognize or if you are suspicious that the email could be a hoax.

Email and Internet Security
Spam

Email spam is unsolicited messages sent to numerous recipients, similar to junk mail.

- Spam is dangerous because it can contain links that direct you to phishing websites or install malware on your computer.
- Studies estimate that between 70% and 95% of emails sent are spam.

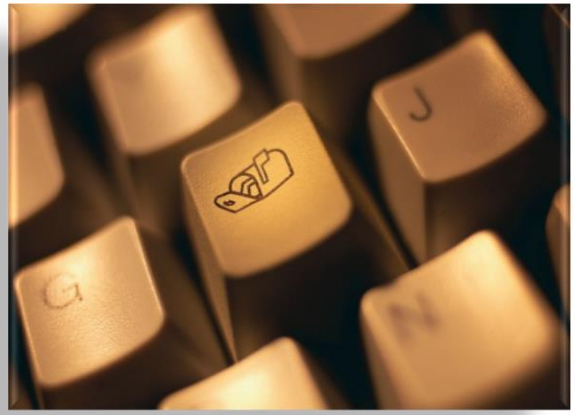
Combat spam

- **NEVER** click on links or download attachments from spam email
- Only provide your email address for legitimate business purposes.
- Do not sign web site guest books and limit mailing list subscriptions. Spammers access these to obtain your email address.
- Spam received in your government email account should be forwarded to the security POC or spam@hhs.gov.

Email and Internet Security
Appropriate Use of Email

CMS email accounts are for official business.

Employees are permitted limited personal use of email.



- Personal emails should not:
  - Disrupt employee productivity;
  - Disrupt service or cause congestion on the network. For example sending spam or large media files; and/or
  - Engage in inappropriate activities.
- Review the *HHS Rules of Behavior (For Use of Information Technology Resources)* for more information.
- Emails that contain sensitive data must be encrypted before being sent.

Email and Internet Security
Peer to Peer Software

- Peer to peer, or P2P, is typically used to download copyrighted files like music. Downloading files in this manner is illegal, unethical and prohibited on government-owned computers and networks.

- Some P2P software may be necessary to meet a business need, in which case you may use it, but only with permission from the CMS CIO. Speak to your manager for more information.

Email and Internet Security
Cookies

A cookie is a text file that a website puts on your hard drive that saves information that you typed in like preferences or user name.

- Cookies can also be used to track your activities on the web.
- Cookies pose a security risk because someone could access your personal information or invade your privacy.

Combat cookies

- Use cookies with caution.
- Confirm that web sites that ask for personal information are encrypted and the URL begins with “https”.
- Note that there is an inherent risk anytime you enter personal information on a web site.

Email and Internet Security
ActiveX

- ActiveX is a form of mobile code technology that allows Internet browsers to run small applications online.
- They pose a security risk because the code alters your computer's operating system. This is a problem if the code is malicious.

Protect your computer

- Require confirmation before enabling ActiveX or other types of mobile code technology.

Email and Internet Security Knowledge Check

A phishing email:

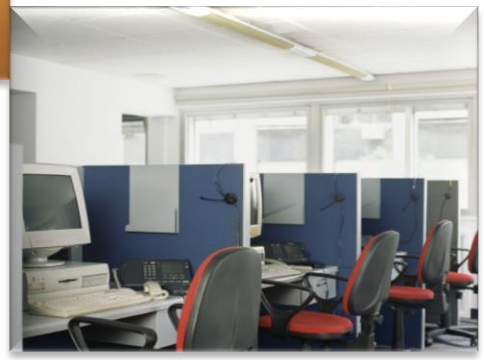
- A: Is a type of social engineering attack.
- B: Can be from an organization that you recognize, like a professional association.
- C: Contains a link to a web site that asks you for personal information.
- D: All of the above.

Email and Internet Security Knowledge Check - Answer

The correct answer is:

- Phishing emails are social engineering attacks.
- The emails seem like they are sent from an organization that you know and trust like a financial institution or professional association.
- Phishing emails always ask for personal information.

Security Outside of the Office



Security Outside of the Office
Travel

✓ **Objective:** Identify best practices to secure IT assets and data in and out of the office.

Technology, telework, and job duties mean that many employees regularly work away from the office.

Be vigilant about protecting information and information systems outside of the office.

Security Outside of the Office
Protect Information Systems While on Travel

- Always maintain possession of your laptop and other mobile devices.
- Ensure that the wireless security features are properly configured.
- Be cautious when establishing a VPN connection through a non-secure environment (e.g., hotel). Do not work on sensitive material when using an insecure connection.
- Turn off/disable wireless capability when connected via LAN cable.
- Turn off your laptop while travelling so that encryption is enabled.
- Report a loss or theft of your laptop or other government furnished device immediately to the CMS IT Service Desk.

Security Outside of the Office Telework

You must receive approval and satisfy CMS requirements for telework. For more information see the:

- *HHS Rules of Behavior (for Use of Information Technology Resources)*
- *CMS-OCIO Policy for Personal Use of Information Technology Resources*
- *CMS Policy for Information Technology Security for Remote Access*.

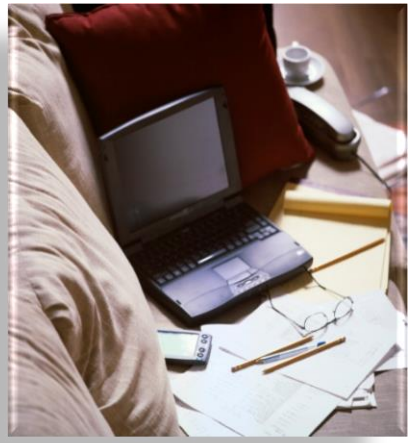
Protect information and data while teleworking

- Always keep your laptop in sight to prevent loss or theft.
- Only use authorized equipment in authorized locations.
- Use a screen protector so sensitive information cannot be seen by others.
- Report lost or stolen equipment immediately.

Security Outside of the Office
Home Security

Many of the tips in this course can be used to protect your home computer.

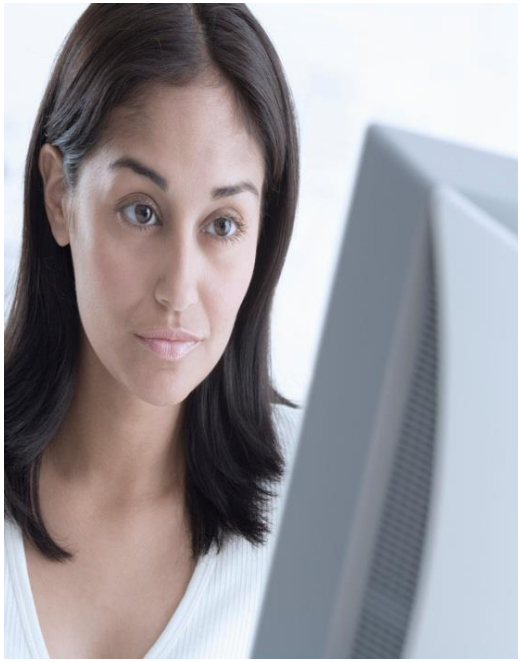
- Criminals can use your personal information to steal your identity and ruin your finances.
- Protecting yourself and your family on the Internet at home is just as important as protecting information systems at work.



Follow these important steps to safeguard your home computer

- Use passwords on personal computers and mobile devices.
- Install and update antivirus software on your home computer.
- Enable the firewall on your computer.
- Routinely backup your files.
- Follow the instructions in the user manual to enable encryption for your wireless router.

Privacy



Privacy
What is Privacy?

✓ **Objective:** Define privacy and PII

Privacy is a set of fair information practices to ensure:

- Personal information is accurate, relevant, and current.
- All *collections*, uses, *and disclosures* of personal information are known and appropriate.
- Personal information is protected.

Privacy enables trust between CMS and the American public.

Successfully achieving CMS' mission depends on protecting personally identifiable information from loss, theft, or misuse.

Key Privacy Guidance and Policy

Guidance

Office of Management and Budget (M) 07-16: Requires safeguards for PII in electronic or paper format and policies and procedures for privacy incident reporting and handling.

Policy

– ***CMS Policy for Information Security and Privacy:*** *Implements procedures and controls at all levels to protect the confidentiality and integrity of information stored and processed on our systems.*

Fair Information Practice Principles

In 1973, HHS advanced the notion of the Fair Information Practice Principles (FIPPs).

These principles are the foundation for privacy protections and compliance frameworks at HHS and across the government.

Privacy Framework*

1. Transparency
2. Individual Participation and Redress
3. Purpose Specification
4. Data Minimization and Retention
5. Use Limitation
6. Data Quality and Integrity
7. Security

* Federal Enterprise Architecture-Security and Privacy Profile (FEA-SPP).

What is Personally Identifiable Information (PII)?

"…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..."*

* OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

Putting Privacy into Action

Everyday, CMS employees support these principles and the commitment they represent.

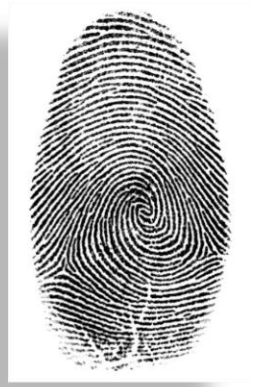
Framework	Description	
Data Minimization and Retention	CMS collects PII that is directly relevant and necessary to accomplish the specified purpose(s) and that PII should only be retained for as long as necessary to fulfill the specified purpose(s) and in accordance with the National Archives and Records Administration (NARA) approved record retention schedule.	▪ Collecting minimum data on forms ▪ Redacting records ▪ Truncating data elements ▪ Records are maintained and destroyed per NARA guidance
Use Limitation	CMS uses PII for the purpose(s) specified in the public notice and data should not be disclosed, made available or otherwise used for purposes other than those compatible with the purpose(s) for which the information was collected except with the consent of the data subject; or by the authority of law.	▪ PII collected for determination of benefits is not used for marketing
Transparency	CMS provides a notice to individuals regarding the collection, use, dissemination, and maintenance of PII.	

Putting Privacy into Action (cont…)

Framework	Description	Examples
Individual Participation and Redress	Individuals provide *CMS* with consent for the collection, use, dissemination, and the maintenance of PII and HHS has appropriate mechanisms for access, correction, and redress regarding the use of their PII.	▪ Individuals can request to review information about them maintained in a System or Record ▪ Individuals can request that errors to be corrected (redress)
Purpose Specification	*CMS* provides the purpose for which the PII is collected at the time of collection, how the PII will be used, and the authority that permits the collection of PII.	▪ Privacy Act Statements ▪ System of Records Notices in Federal Register
Data Quality and Integrity	*CMS uses PII that is accurate, relevant, timely and complete for the purposes for which it is to be used.*	▪ PII updates records and seeks clarification from individuals (as needed)
Security	*CMS* protects PII, in all formats, through administrative, technical, and physical security safeguards which guard against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.	▪Encryption ▪Shredding ▪User Names and passwords ▪Locks

Privacy
Common Examples of PII

- Name
- Social Security number (SSN)
- *Health Insurance Claim Number*
- Date of birth (DOB)
- *National Provider Identification (NPI) Number*
- Driver's license number
- Passport number
- Personal Health Information (PHI)
- *Biometric Information*



Privacy
PII in Context

What is the chance that you can successfully identify a person with only this information?

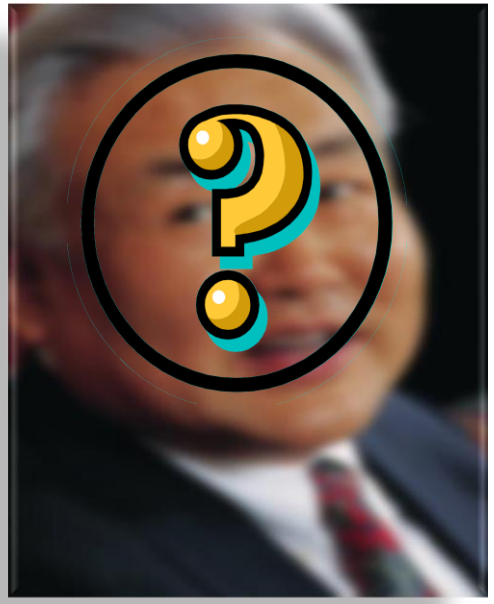
Mr. X lives in ZIP code 02138 and was born July 31, 1945.

A) 1%

B) 87%

C) 50%

D) 34%



(Source: "What Information is 'Personally Identifiable?", Electronic Frontier Foundation by September 11, 2009.)

The answer is **B**. Latanya Sweeney, a Carnegie Mellon University computer science professor, demonstrated that a person's gender, zip code, and date of birth could be used to identify an individual 87% of the time.

Privacy: PII in Context

Seemingly innocuous information can identify an individual when combined with other data or compared to a data set that includes other PII. Professor Sweeney compared the list of gender, zip codes, and dates of birth with voter registration records for her research.

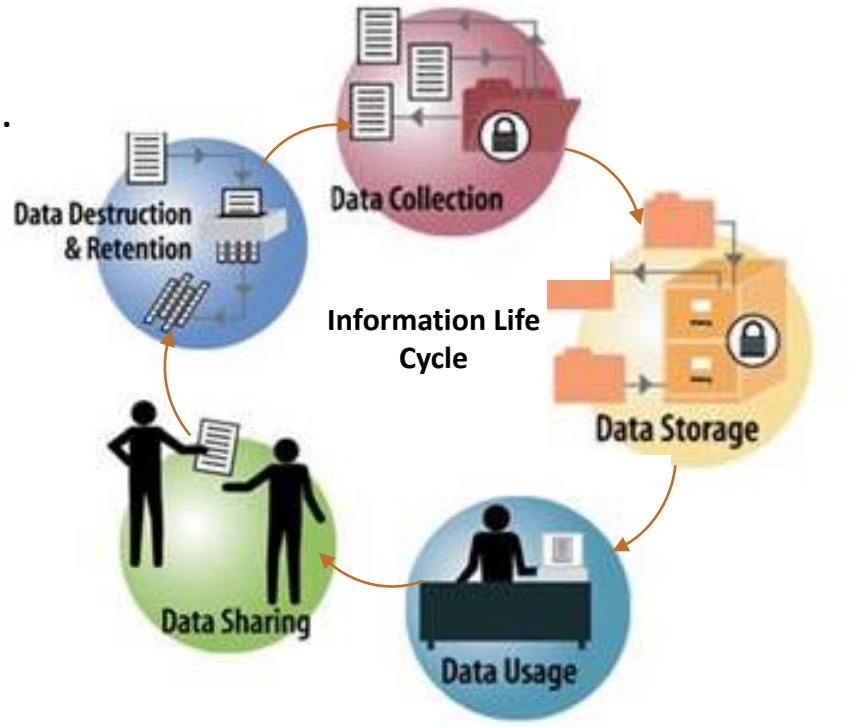
PII must be protected at all times even if the information cannot be used singularly to identify individuals.

Information Life Cycle

Privacy is important during each stage of the information life cycle:

- Collection: Gathering PII for use.
- Storage: Maintaining or storing PII.
- Use: Using PII to accomplish a job function.
- Sharing: Disclosing or transferring PII.

- Destruction and Retention: Destroying or maintaining equipment, media, or documents containing PII.



Privacy Considerations

Are you allowed to collect the PII by law?

Do you have a legitimate business need to collect the PII?

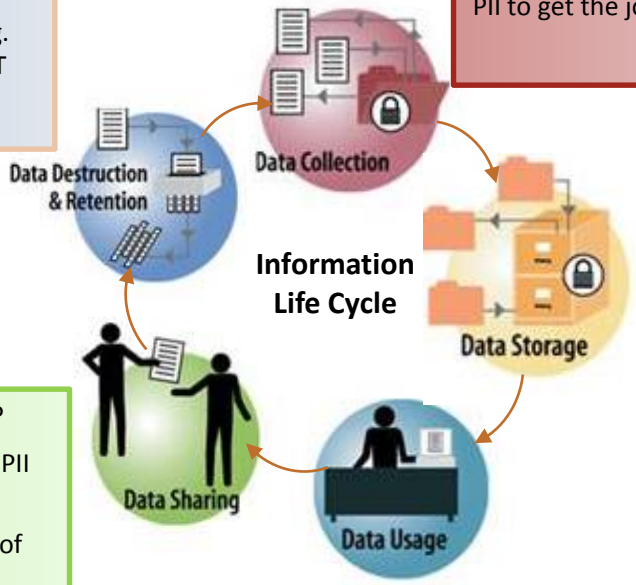
Are you obtaining it in a safe manner so that it cannot be overheard or seen by others?

Did you only request the minimum amount of PII to get the job done?

Is the PII part of a record that falls under the records retention schedule?

Did you shred all papers containing PII?

Did you give back unused equipment (e.g. computer, copiers, fax machines) to the IT Department for proper disposal?



Did you secure documents and files that contain PII?

Are you storing PII on only authorized portable electronic devices (i.e., work equipment)?

Did you follow proper security procedures to secure the stored PII (e.g., encryption)?

Did you verify that the sharing is allowed?

Have you verified that everyone that the PII is being shared with has a need to know?

Did you share only the minimum amount of PII and follow disclosure procedures?

Did you share using the appropriate safeguards (e.g., encryption)?

Will you use the PII for the purpose it was provided?

Are you only using the minimum amount of PII to get the job done?

Are you accessing PII through secure and authorized equipment or connections?

Privacy Spillage

✓ **Objective:** Recognize threats to information systems and privacy

Spillage is the improper storage, transmission or processing of PII.

Combat spillage

- Share information on a need to know basis.
- Never access PII unless authorized to do so to perform your job.
- Only store PII on encrypted devices.
- Encrypt emails and double-check that the recipient name(s) is correct before sending.
- When faxing, confirm that you have the correct fax number and call the recipient to confirm receipt.

Protect PII: SSN *and HICN* Protections

CMS Users that handle SSNs *and HICNs* need to take precautions. Misuse of SSNs *and HICNs* can put individuals at risk for identity theft.

CMS Users should:

- Use the SSN *and HICN* only when it is required.
- Truncate or mask the SSN *and HICN* in systems or on paper printouts whenever possible.
- Disclose SSNs *and HICNs* to those that have need know and are authorized to receive the information.
- Documents containing SSNs *and HICNs* should be locked up and put away so they are not left out when away from your desk.
- Identify and implement ways to eliminate the use of SSNs *and HICNs* (e.g., removal from forms, assigning a randomly generate identifier).

Privacy
Roles and Responsibilities

✓ **Objective:** Understand personal responsibility to protect information systems

As a member of the CMS workforce, you are responsible for following privacy policies and procedures.

Privacy policies and procedures require you to:

- Collect, use, and disclose personal information for reasons that are for a legitimate job function, support the mission of CMS, and are allowed by law.
- Disclose only the minimum amount of information.
- Access information only for authorized purposes.
- Follow standards to safeguard personal information throughout the information life cycle.
- Report suspected privacy violations or incidents.
- Comply with all applicable privacy laws.
- Shred documents containing PII; NEVER place them in the trash. Contact the IT Department for proper disposal of equipment like copy machines and computers.

Privacy
Consequences of Privacy Violations

Privacy violations can result in severe consequences including:

Employee discipline

Fines

Imprisonment

Privacy Knowledge Check

True or False. Only PII that can be used to directly identify an individual needs protection.

Privacy
Knowledge Check - Answer

The correct answer is:

Seemingly harmless PII, like gender or a spouse's name, can still be used to identify a person and must be protected.

Incident Reporting

Incident Reporting
Privacy & Data Breaches

✓ **Objective:** Identify the correct way to respond to a suspected or confirmed security or privacy incident.

- Privacy and data breaches can result in:
  - Inability for CMS to fulfill its mission;
  - Disruption of day-to-day operations;
  - Damage to the reputation of CMS; and
  - Harm to an individual's health or financial status.
- In the case of data being lost, stolen or misused, it is important to know how to respond.

A prompt and correct response could limit the severity of the breach and protect privacy of individuals.

What is a Breach of Privacy?

"the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar terms referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic."*

* OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

Incident Reporting
Common Scenarios

Common scenarios when an incident should be reported include:

- Loss, damage, theft, or improper disposal of equipment, media, or papers containing PII.
- Accidentally sending a report containing PII to a person not authorized to view the report or sending it in an unprotected manner (e.g., unencrypted).

- Allowing an unauthorized person to use your computer or credentials to access PII.
- Discussing work related information, such as a person's medical health records, in a public area.
- Accessing the private records of friends, neighbors, celebrities, etc. for casual viewing.
- Any security situation that could compromise PII (e.g., virus, phishing email, social engineering attack).

Incident Reporting - Report an Incident

- Do not investigate the incident on your own - *immediately* report suspected incidents, especially those that could compromise PII, regardless of whether it is in electronic, paper, or oral format.

  Report incidents to CMS IT Service Desk:

  1-800-562-1963 /410-786-2580 or

  cms_it_service_desk@cms.hhs.gov

- Any employee can report an incident. You are not required to speak to your manager before reporting an incident but should keep management informed when incidents occur.

Incident Reporting Knowledge Check

Amy left her laptop in a taxi cab on the way to the airport. What should she do? *(choose the best answer)*

- A: Nothing. The files were backed up anyway.
- B: Cancel the trip.
- C: Report the laptop missing to the CMS IT Service Desk.
- D: Buy a new laptop as a replacement.

Incident Reporting Knowledge Check - Answer

The correct answer is:

Contact the CMS IT Service Desk as soon as you notice a laptop or other mobile device missing or stolen.

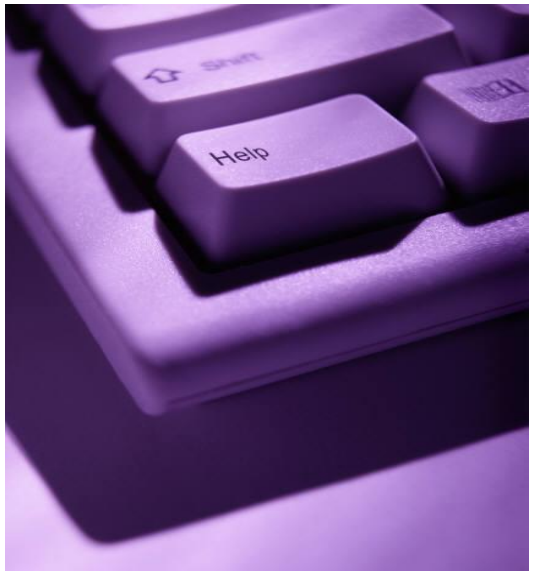
Summary

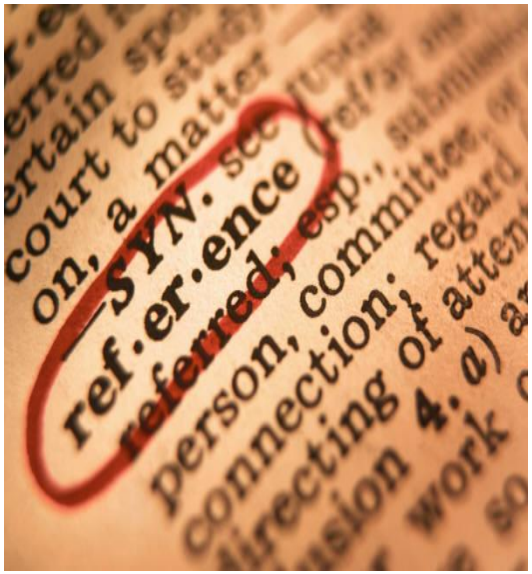
Summary - Objectives

You should now be able to:

- ✓ Define information systems security;
- ✓ Identify federal regulations that mandate the protection of IT assets;
- ✓ Understand CMS' IT security and privacy policy, procedures, and practices;
- ✓ Understand personal responsibility to protect information systems and privacy;
- ✓ Recognize threats to information systems and privacy;
- ✓ Identify best practices to secure IT assets and data in and out of the office;
- ✓ Define privacy and personally identifiable information (PII); and
- ✓ Identify the correct way to respond to a suspected or confirmed security or privacy incident.

Appendix


Help


SYN.
ref.er.ence
referred; esp.,
person, committee,
connection; regard
directing of atten
4. a)
work

Appendix

CMS Information Security and Privacy Program

Resources

- Information pertaining to the HHS Information Security Program can be found at: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html

- Information pertaining to the CMS Information Security Privacy Program policy guidance, standards, regulations, laws, and other documentation: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

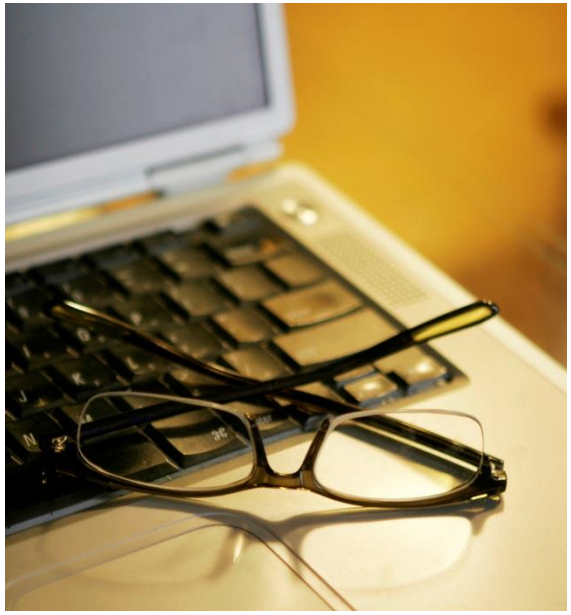
- Information pertaining to the CMS Privacy Program can be found at: https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/index.html

Appendix
Privacy Points of Contact

- For specific security and privacy-related questions, contact:
- privacy@cms.hhs.gov or call 410-786-5357
- OpDiv Senior Official for Privacy (SOP) http://intranet.hhs.gov/it/cybersecurity/policies/index.html
- Privacy Act Contacts http://www.hhs.gov/foia/contacts/index.html

Acknowledgement of HHS Rules and Behavior

On the next slide, you will read and acknowledge the HHS Rules of Behavior.



HHS Rules of Behavior and Acknowledgement

Please click on the following link to review the HHS Rules of Behavior:
http://www.hhs.gov/ocio/policy/hhs-rob.html

Remember to be sure to print the Rules of Behavior for future reference.

Congratulations!

You have completed the **Information Systems Security and Privacy Awareness!**


CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF ENTERPRISE SERVICES