CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION TECHNOLOGY

Information Systems Security and Privacy Awareness Training

Information Security & Privacy Group (ISPG)

Office of Information Technology (OIT)

Welcome

“Welcome. 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 annual Federal Information Security Management Act (FISMA) requirement for security and privacy awareness training for users of Federal information systems.

This course will take approximately 60 minutes to complete.

Later in this training, you will need to read and acknowledge the HHS Rules of Behavior to achieve course completion.

Let’s get started. Cybersecurity in the workplace is everyone’s business.”

Privacy is Paramount

Privacy enables trust between CMS and the American public.

CMS is entrusted with the Personally Identifiable Information (PII) and Protected Health Information (PHI) of nearly **150 million** Americans, nearly **45%** of the U.S. population.

- Authority to collect
- Limitations on use
- Data retention minimization policies to follow

Successfully achieving the CMS mission depends on protecting sensitive information of all kinds from loss, theft, or misuse.

Topic 1: Define Privacy, PII and PHI

- ✓ **Objective 1:** Define Privacy, Personally Identifiable Information (PII), Protected Health Information (PHI) and Sensitive Information (SI).
- ✓ **Objective 2:** Identify types of PII, PHI and SI and recognize what makes them different.

What Is Privacy?

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

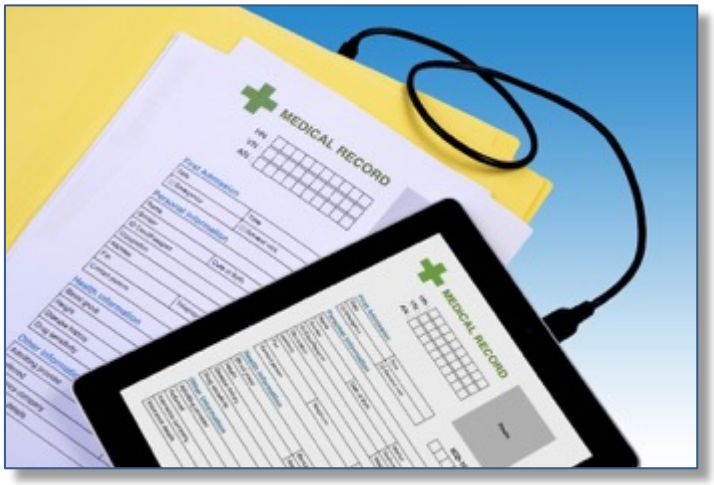
How can we accomplish these Privacy goals?

What are PII and PHI?

Personally Identifiable Information (PII)

means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

OMB Circular No. A-130 , *Managing Information as a Strategic Resource* (July 28, 2016)



Protected Heath Information (PHI)

means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, transmitted or maintained in any other form or medium.

HIPAA Privacy Rule at 45 CFR § 160.103

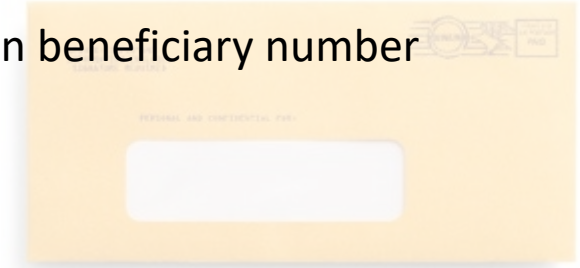
Examples of PII and PHI

Personally Identifiable Information

- Name
- Social Security Number
- Date of Birth
- Photograph
- Fingerprint
- Personal mailing or email address
- Taxpayer identification number

Protected Health Information

- Patient identification number
- Medicare beneficiary number (MBI)
- Dates — including birth, discharge, admittance, and death dates.
- Medical notes
- Prescription information
- Health plan beneficiary number



PII & PHI must be protected in any form – paper, electronic, oral.

What Is SI?

Sensitive Information (SI)

"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 conduct of HHS programs, or the privacy of individuals entitled under The Privacy Act or the Health Insurance Portability and Accountability Act (HIPAA)."

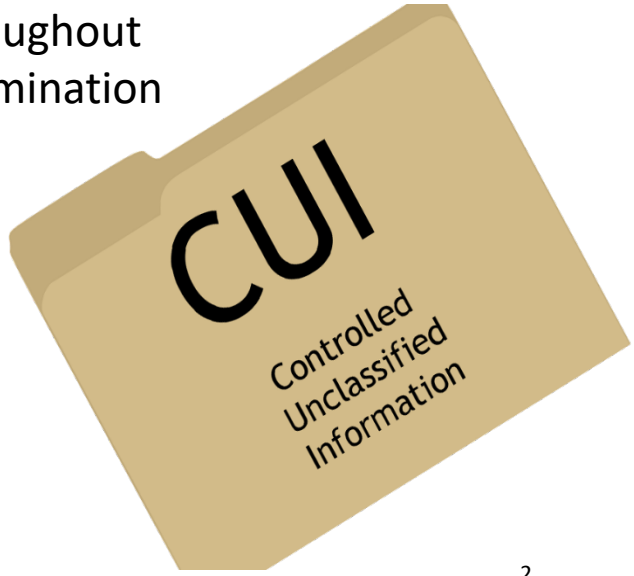
HHS Memo: Updated Departmental Standard for the Definition of Sensitive Information, May 2009

Controlled Unclassified Information (CUI)

Per Executive Order 13556[1]., CUI is defined as "exclusive designations for identifying unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies."

Examples may include but are not limited to:

- Personal Information
  - Personally Identifiable Information (PII)
  - Protected Health Information (e-PHI or PHI)
- Contract Proprietary Information
- Security information
- Proprietary Business Information
- Law Enforcement Investigation Information



What is CUI?[2]

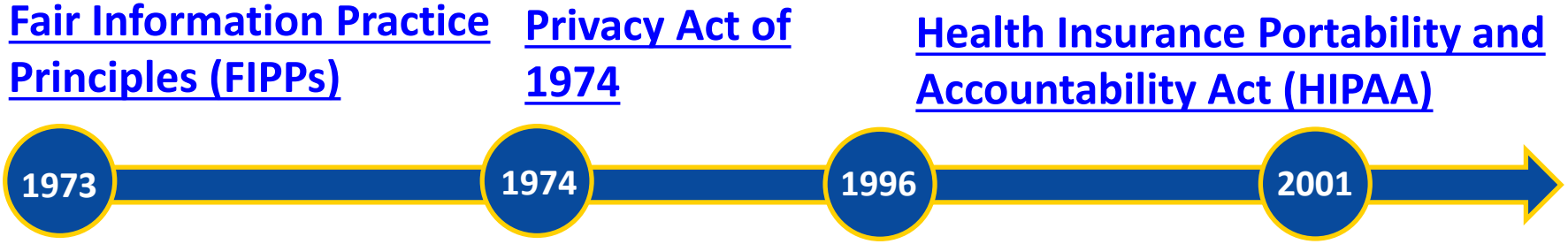
1 – https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information
2 - https://www.archives.gov/files/cui/documents/2011-what-is-cui-bifold-brochure.pdf

Topic 2: Federal Privacy Guidance

✓ **Objective:** Recall the Federal Privacy Authorities.

Timeline of Federal Privacy Authorities

Click the links to learn more.



FIPPS principles are the foundation for privacy protections and compliance across the federal government.

The Privacy Act applies to records about individuals in the possession and control of Federal agencies.

HIPAA's purposes include insurance portability and Administrative Simplification provisions.

The Privacy Rule standards address the use and disclosure of individuals' health information-called "protected health information" by organizations subject to the Privacy Rule – called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used.

FIPPS (Fair Information Practice Principles)

In 1973, HHS released FIPPs. These principles are the foundation for privacy protections and compliance frameworks at HHS and across the government. FIPPs are defined as:

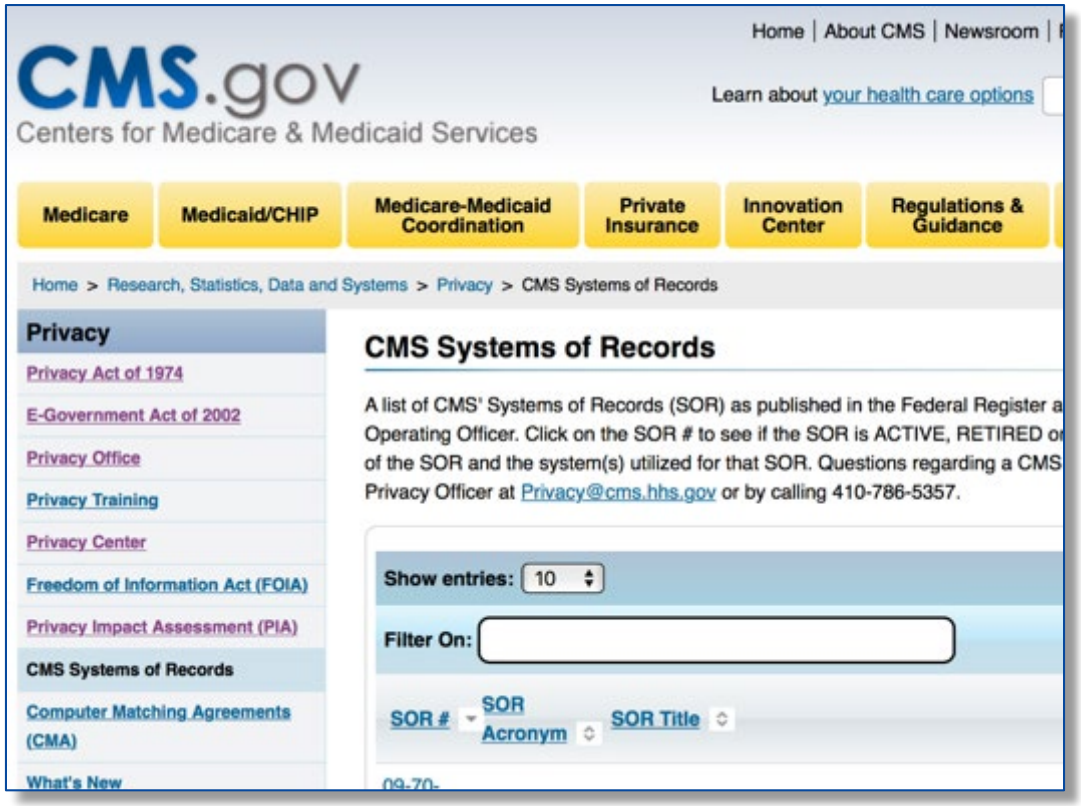
Privacy Act of 1974

For more information visit:
https://www.justice.gov/opcl/privacy-act-1974

- An individual is entitled access to his or her records and to request correction of these records as applicable.
- The Privacy Act prohibits disclosure of these records without an individual's written consent unless one of the twelve disclosure exceptions enumerated in the Act applies.

System of Record Notices (SORNs)

- Records are held in Privacy Act Systems of Records (SOR). A notice of any such system, or SORN is published in the Federal Register.
- These notices identify the legal authority for collecting and storing the records, individuals about whom records will be collected, what kinds of information will be collected, and the routine uses for the records.



For more information visit CMS Systems of Records
https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/CMS-Systems-of-Records.html

Topic 3: Your Role In Protecting Privacy

✓ **Objective:** Recognize your personal responsibility to protect Privacy.

Your Role in Privacy

As a member of the CMS workforce, you are responsible for following all privacy policies and procedures. You are required to:

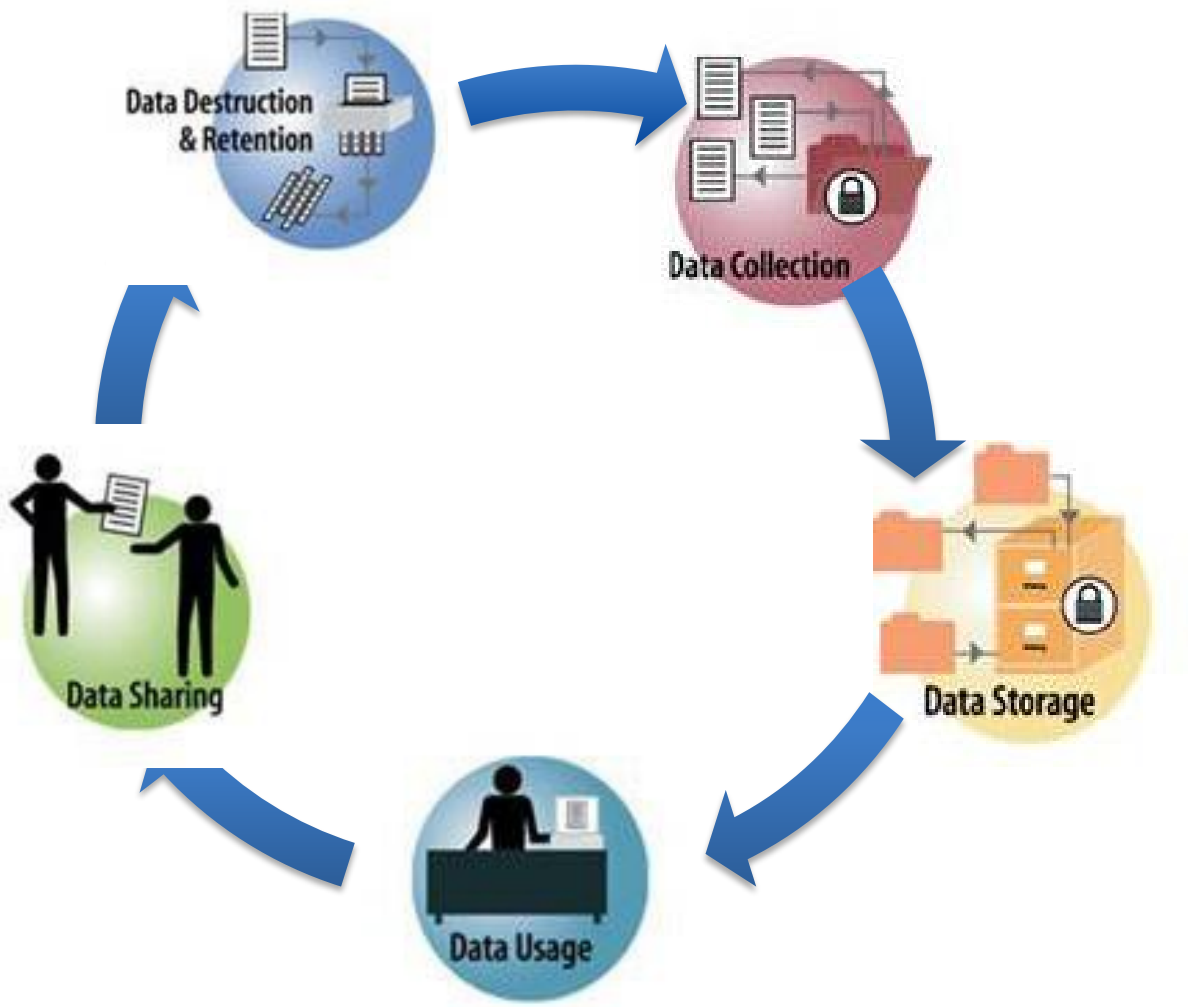
- Collect, use, and disclose personal information **ONLY** for reasons that support legitimate job functions, support the mission of CMS, and are allowed by law
- Disclose only the minimum amount of information
- Access information for authorized purposes ONLY
- Follow standards to safeguard personal information throughout the information life cycle
- Report suspected and actual privacy violations or incidents
- Comply with all applicable privacy laws

Failure to comply puts beneficiaries at risk and can result in severe consequence including disciplinary actions, termination of employment, fines and/or imprisonment.

Questions? Email CISO mailbox: ciso@cms.hhs.gov

The Privacy Lifecycle and You

Privacy is important during each stage of the information life cycle. It is your responsibility to protect privacy from Data Collection to Data Destruction & Retention.



Knowledge Check

Check your Understanding

Let's review the information covered in this module with a few questions.

- These questions are for review only and will not be graded.
- Feedback will be provided for each question.
- Select **Next** when you are ready to begin.

Knowledge Check

Question 1

Which of the following are considered Personally Identifiable Information (PII)? (Select the best answer.)

A. Medical notes
B. Prescription information
C. Photograph
D. Personal mailing or email address
E. Military status
F. All of the above

Knowledge Check

Question 1 Answer

Which of the following are considered Personally Identifiable Information (PII)? (Select the best answer.)

A. Medical notes
B. Prescription information
C. Photograph
D. Personal mailing or email address
E. Military status
F. All of the above

All of these items are a form of personal information, whether PII or PHI. While seemingly innocuous, these types of information can identify an individual when combined with other data or compared to a data set that includes other PII or PHI.

Knowledge Check

Question 2

Jane Smith, an employee of CMS, is working on a report for her manager. It is faster for Jane to pull existing patient data from another report than create a new one. The existing report also contains Social Security numbers and birthdates, information Jane does not need. Is it okay for Jane to use the report to save time?

A. Yes
B. No

Knowledge Check

Question 2 Answer

Jane Smith, an employee of CMS, is working on a report for her manager. It is faster for Jane to pull existing patient data from another report than create a new one. The existing report also contains Social Security numbers and birthdates, information Jane does not need. Is it okay for Jane to use the report to save time?

A. Yes

B. No

CMS personnel can only access information as needed to perform their job and for authorized purposes only.

Information Security Awareness (ISA)

Information Security

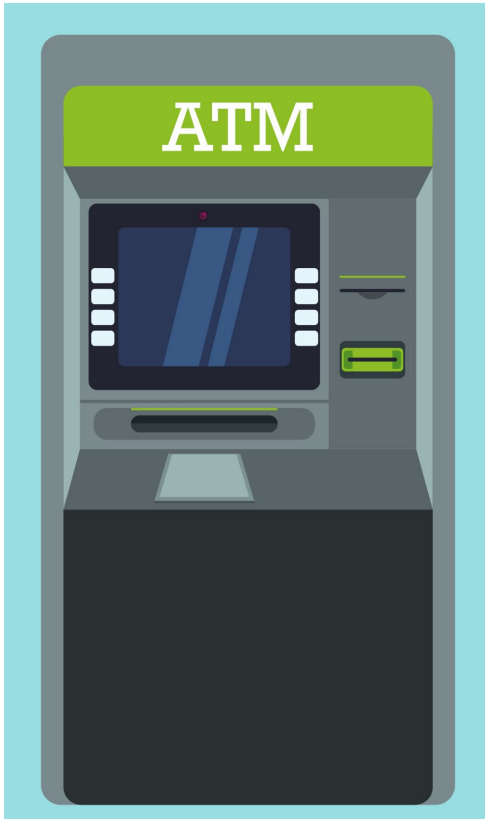
Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

CIA - Confidentiality, Integrity and Availability

Information Security encompasses:

- **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.

What If?



Confidentiality:

What if your account was not kept private and someone else was able to access it when they approached the ATM. How much damage could be done?

Integrity:

What if every time you went to the ATM, the balance it displayed was inaccurate. How could the poor reliability of your balance information adversely affect your account management?

Availability:

What if your bank's ATM was rarely available when you needed it. Would you continue to use that bank?

Threats & Vulnerabilities

Threats – the potential to cause unauthorized disclosure, use, changes, or destruction to an asset. Threats can be natural, such as weather events, or man-made, such as carelessness.

- **Non-Malicious:** A staff person who is unaware or not paying enough attention to required policies and procedures or a person who is aware of required policies and procedures, but chooses to neglect them, assuming that his/her behavior will not have a noticeable impact. Many data breaches are caused by staff, and over half are considered preventable.
- **Malicious:** A person intentionally disrupts, threatens, or endangers CMS activities or assets.

Vulnerabilities – any flaw or weakness, in system operation or personnel behavior, that can be exploited and could result in a breach or a violation of a security or privacy policy.

Insider Threats

Insider Threats – Is a person, known or suspected, who uses their authorized access to CMS facilities, systems, and information to damage the Department or US National Security. Such threats are usually attributed to employees or former employees, but may also arise from third parties, including contractors, temporary workers or customers.

Although no single indicator provides conclusive proof or evidence that an individual is an insider threat, the following depicts some indicators that might be associated with potential insider threats:

1. Disclosure, removal, or unauthorized access of sensitive information without approval.
2. Compromising Personally Identifiable Information / Protected Health Information.
3. Unexplained access to financial resources.
4. Threats of workplace violence or inappropriate conduct towards fellow employees.
5. Express support or action to an institutions, or individuals associated with terrorism.
6. Violations of organizational policies, procedures, and directives.

Report insider threat concerns to the CMS Insider Threat Program at insiderthreat@cms.hhs.gov

Risk

Risk – the likelihood that a threat will exploit a vulnerability. For example, a system may not have a backup power source; making it vulnerable to a threat, such as a thunderstorm, which creates a risk.

Threats + Vulnerabilities = Risk

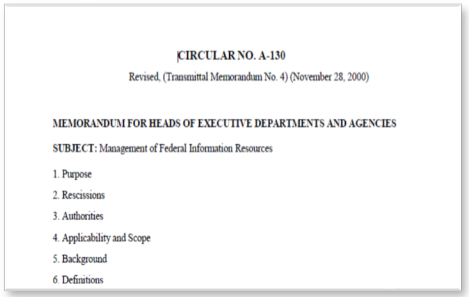
Topic 2: Federal Guidance

✓ **Objective:** Recall the 3 Federal Acts and Guidance on information security.

Federal Guidance

CMS Security is informed, guided, and required by Federal Acts and Guidance. Click here to learn more.

- Office of Management and Budget (OMB) Circular A-130. Click here to learn more.
- E-Government Act of 2002. Click here to learn more.
- Federal Information Security Modernization Act of 2014. Click here to learn more.



CIRCULAR NO. A-130

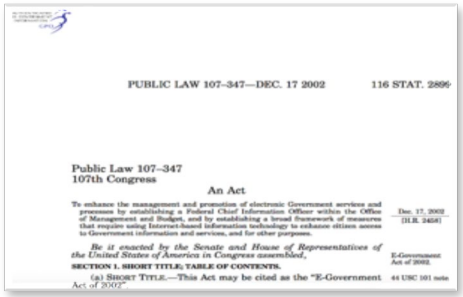
Revised. (Transmittal Memorandum No. 4) (November 28, 2000)

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Management of Federal Information Resources

1. Purpose
2. Rescissions
3. Authorities
4. Applicability and Scope
5. Background
6. Definitions

Office of Management and Budget (OMB) Circular A-130



PUBLIC LAW 107–347—DEC. 17 2002 116 STAT. 2899

Public Law 107–347
107th Congress

An Act

To enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.

Dec. 17, 2002
[H.R. 2458]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

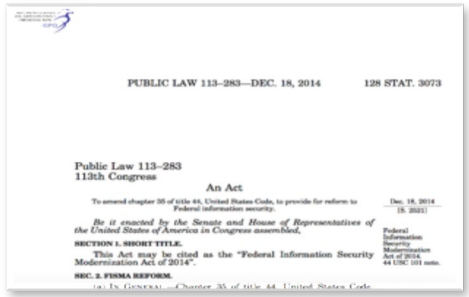
E-Government Act of 2002.

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "E-Government Act of 2002".

44 USC 101 note

E-Government Act of 2002



PUBLIC LAW 113–283—DEC. 18, 2014 128 STAT. 3073

Public Law 113–283
113th Congress

An Act

To amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security.

Dec. 18, 2014
[S. 2521]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Federal Information Security Modernization Act of 2014.
44 USC 101 note.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Federal Information Security Modernization Act of 2014".

SEC. 2. FISMA REFORM.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code

Federal Information Security Modernization Act of 2014

Topic 3: Your Role

✓ **Objective:** Identify your role in information security and privacy protection.

Proper Use of CMS E-Mail Accounts

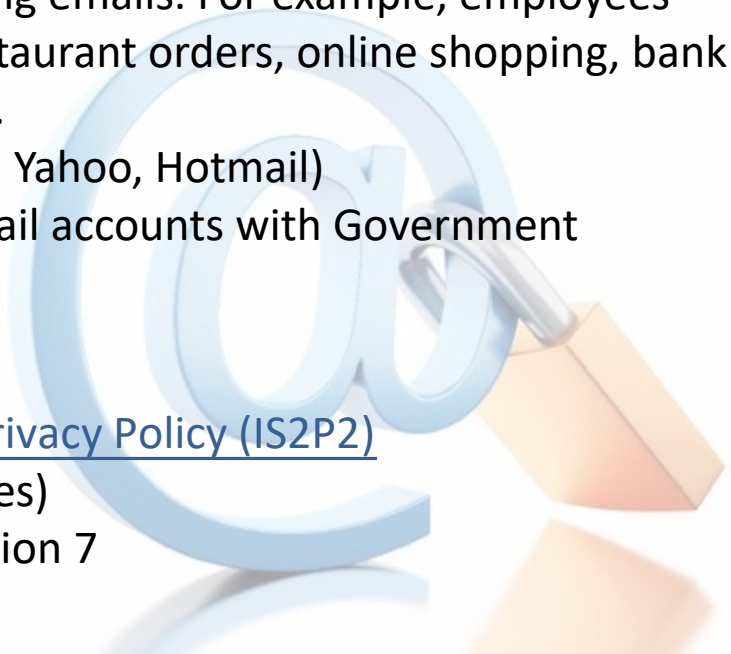
CMS email accounts are for Agency use only.

The following are strictly prohibited:

- Using CMS email addresses for non-work related activities, except as necessary for emergency contact information (e.g., school, day care, adult care facility). Such use increases the risk of receiving spam and phishing emails. For example, employees should not use their CMS email address for restaurant orders, online shopping, bank log-ins, retail flyers, promotional materials, etc.
- Accessing personal email accounts (e.g., Gmail, Yahoo, Hotmail)
- Conducting official business using personal email accounts with Government Furnished Equipment.

For more information, review the following:

- CMS Information Systems Security and Privacy Policy (IS2P2)
- HHS Rules of Behavior (Use of IT Resources)
- Master Labor Agreement, Article 35, Section 7

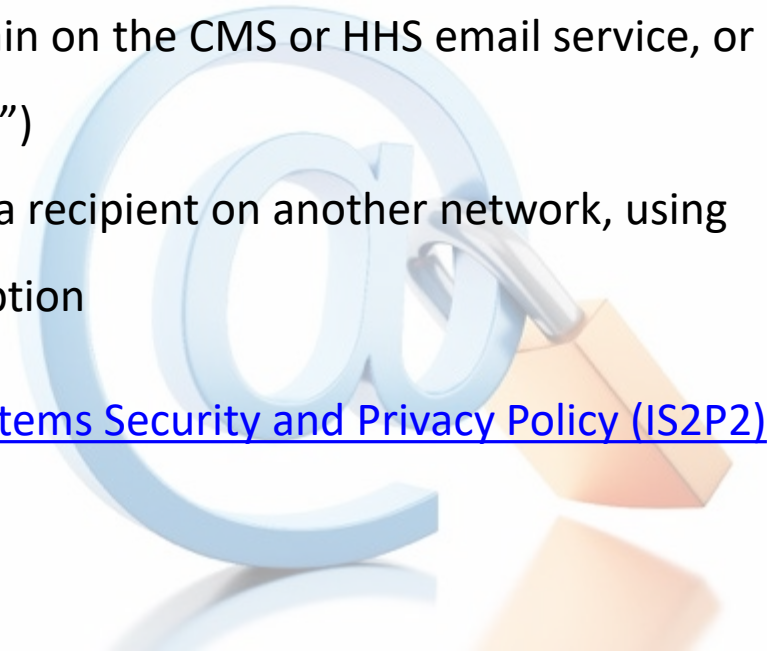


Protect Sensitive Information in E-Mail

CMS Sensitive Information (SI) must be protected as follows:

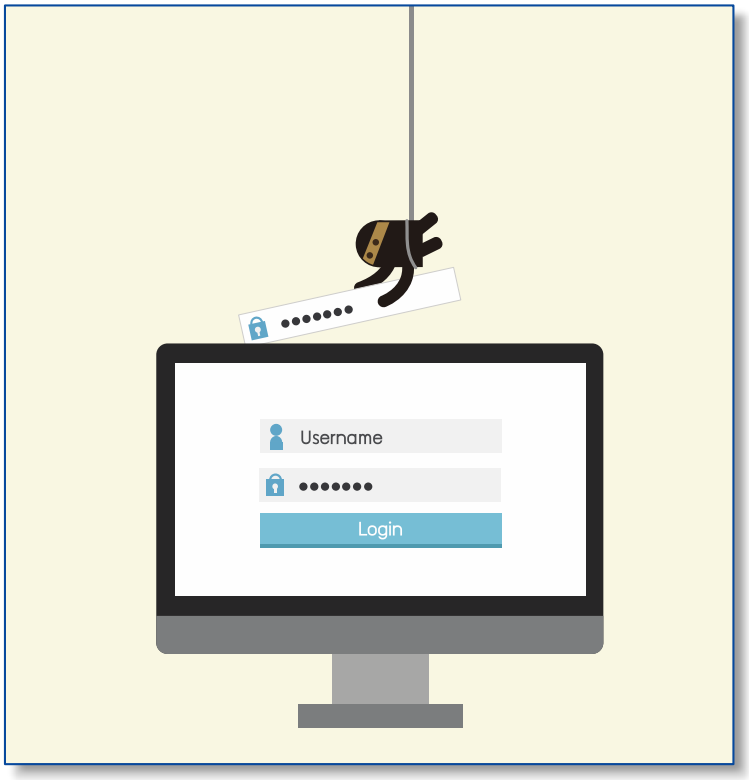
- Only send SI to recipients with a “need to know“
- Ensure unencrypted emails containing SI remain on the CMS or HHS email service, or trusted partner (i.e. “jane.doe@opdiv.hhs.gov”)
- Encrypt emails containing SI when sending to a recipient on another network, using Personal Identity Verification (PIV) card encryption

For more information, review the CMS Information Systems Security and Privacy Policy (IS2P2) (*See CMS Email Encryption Requirements)*.



Password Protection

A strong password for your network account and other applications is a basic protection mechanism.



General password rules:

- Easy to remember or generic word passwords are not secure.
- Passwords should be least eight characters in length.
- Passwords should contain a combination of: Capital and Lowercase letters, Numbers and Symbols.
- Try to commit passwords to memory, **do not** keep written passwords near your computer.

Passphrases

A passphrase is a technique to create a strong but memorable password.

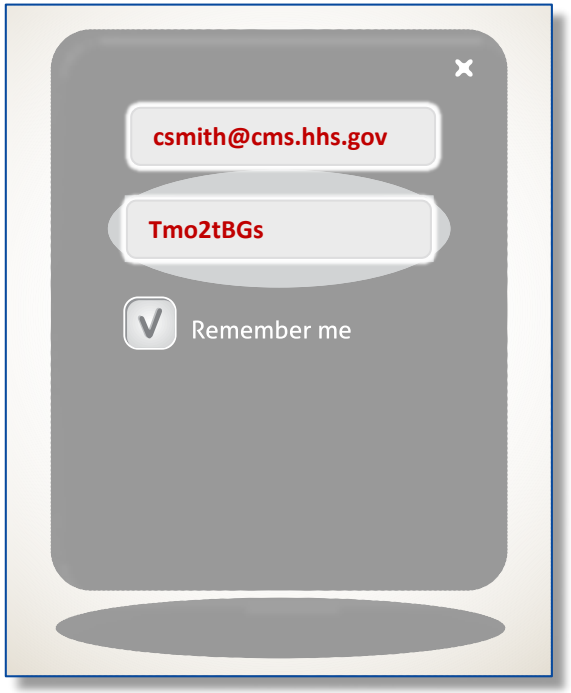
For example:

- Use the initials of a song or phrase to create a unique password.

"Take me out to the ballgame"

becomes

Tmo2tBGs



Password Protection Tips

- Change password often. CMS will remind you to do this, but also 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.
- Do not reuse a password.
- 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.

Encryption

Encryption: 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 PII/PHI have encryption enabled while in transfer and while stored.
- Emails that contain PII/PHI must have encryption enabled before the sender sends them.

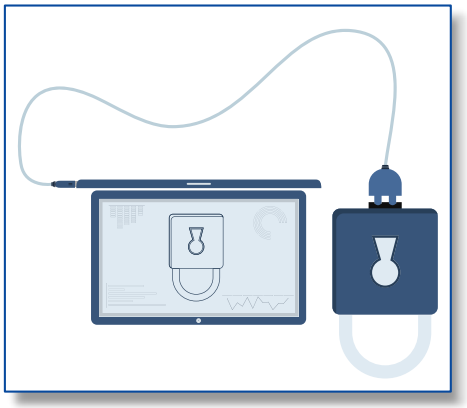
Personal Identity Verification (PIV) Cards

PIV cards contain YOUR digital credentials for gaining access to HHS government buildings/secured areas, encrypting emails, and digitally signing documents.

- 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.

At CMS your PIV card is also your authentication device to access your government-issued computer.

Tailgating



Report any suspicious activity to the security office.

Be wary of tailgating attempts and follow these tips to avoid become a victim:

- Never allow anyone to follow you into the building or a secure area without his or her badge.
- Do not allow anyone else to use your PIV card for building or secure area access.
- Secure your workstation when leaving the office and 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.

Topic 4: Common Types of Attacks

✓ **Objective:** Recognize common threats to information security and privacy.

Social Engineering

- “Social engineering” attempts to manipulate you into unwittingly divulging information to a hacker, or into taking an action that leads to a security or privacy breach.

- 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 CMS information and information systems through you.

- Normal appearing websites that seem to be legitimate may be compromised with malicious links or malware infecting visiting devices.

- ‘Friend Requests’ on social networks may impersonate friends and colleagues to trick you into accepting malware or divulging sensitive information.

Social Engineering Targets

Social engineering attacks target natural human behaviors such as:

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

Social engineering attacks are more common and more successful than computer hacking attacks against the network.

Social Engineers

Social engineers seek information that will give them access to sensitive information.

Common targets include:

- Passwords
- Security badges
- Access to computer systems
- Access to secure areas of the building
- Employee personal information, i.e., PII
- Beneficiary information, i.e., PHI

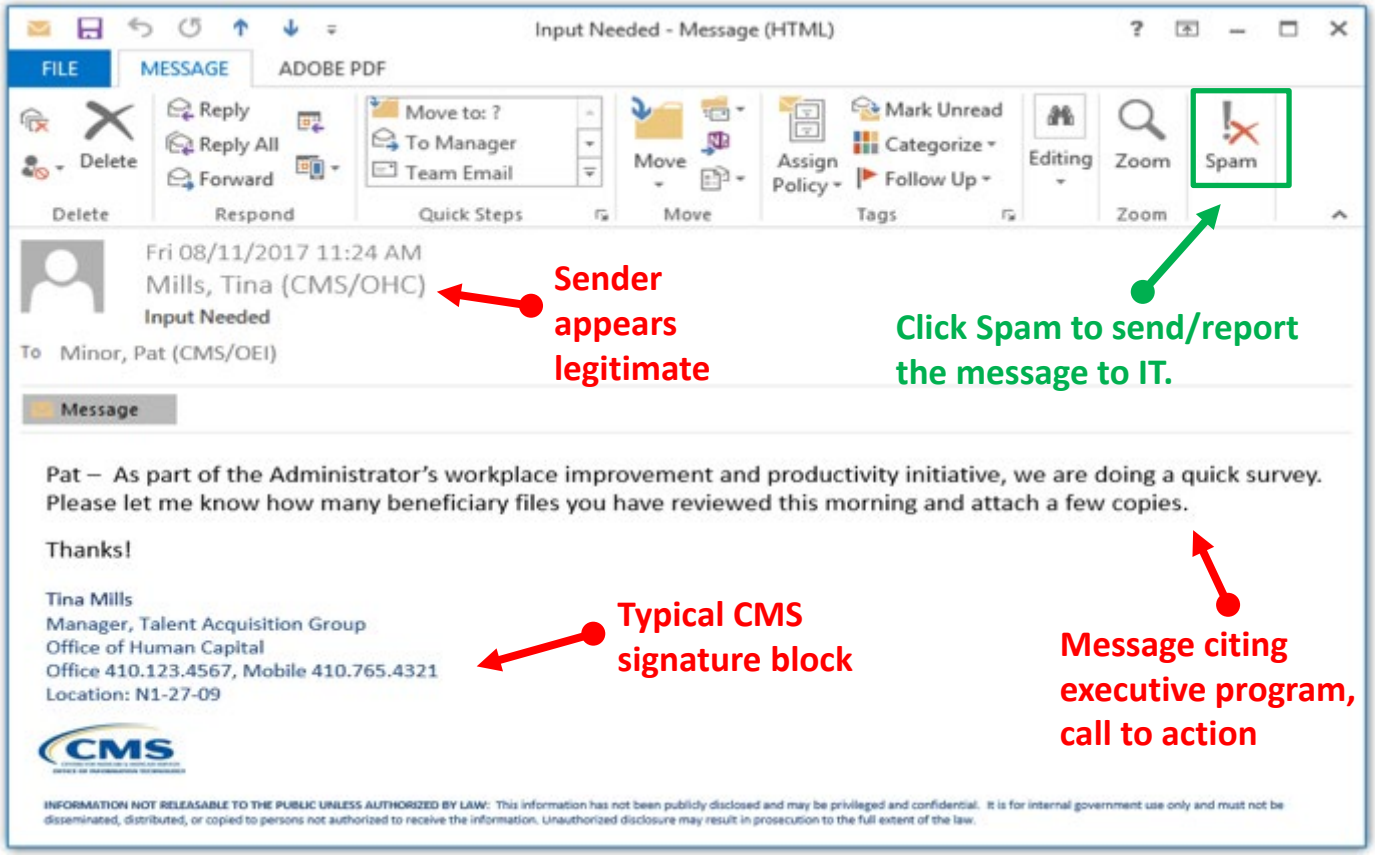
Phishing

Phishing is a form of social engineering whereby intruders seek to gain access to information and information systems by posing as a real person, business or organization with legitimate reason to request the information.

- Phishing emails (or texts) often alert you to a problem with your account and ask you to click on a link to provide information to correct the problem.
- These links 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.
- These emails often look real and appear to contain real organizational logos and trademarks.
- The URL provided may even resemble the authentic URL web address, for example, “Amazons.com” with a very minor spelling error that one could easily overlook.

Spear Phishing

Spear Phishing is a type of phishing attack aimed at a specific individual or business.



A spear phishing email may be personally addressed to you and appear to be sent from a legitimate source you know and trust, like a government agency or a professional association.

Watering Holes

- Hackers sometimes lurk around websites that are known to attract high value individuals, just as lion's prey on animals gathering at a "watering hole" in the wild.
- By prowling the group, hackers sharpen their attack, and when one member is compromised others become more vulnerable.
- In this attack, the selected website may be compromised as a method to target its visitors.
- Without the visitor's knowledge, personal information shared on the website may be stolen by the hacker, while susceptible computers may be infected by malware.

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
- Visiting an infected web site

Malware can corrupt files, erase your hard drive, or give a hacker access to your computer.

Combating Malware

Protect yourself from Malware:

- Read email in plain text, 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.
- Use the Spam button to report suspicious emails without opening them.
- If you believe your computer is infected, contact the CMS service desk.

Topic 5: Securing Assets Outside the Office

✓ **Objective:** Identify best practices to secure information assets when out of the office.

Free Wi-Fi

Free Wi-Fi Networks

- Malicious actors could be lurking in free Wi-Fi networks, such as those at your local coffee shop, airport, etc.

- Do not connect GFE or contractor-owned equipment to unsecured Wi-Fi networks (e.g. airports, hotels, restaurants, etc.) and public Wi-Fi to conduct CMS business…unless the Wi-Fi is at a minimum password protected; at which time you must then connect to VPN prior to accessing your CMS resources.

- Only use secured Wi-Fi networks such as your home Wi- Fi or Hotspot devices (mobile phone/tablet.)

Protecting Information While Traveling

- Always maintain possession of your laptop and other mobile devices.
- 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 traveling so that encryption is enabled.
- Report a loss or theft **immediately** to the CMS Service Desk.

Protecting Information On International Travel

Official (Government Business):
CMS employees and contractors who travel or deploy internationally on behalf of the United States Government are at particular risk in certain parts of the world. The foreign security approval is part of the CONCUR process.

CMS International Team will contact the individual to provide additional information as needed.

Unofficial (Personal Travel)
CMS employees and contractors who wish to take their CMS network accessible devices on unofficial travel are required to receive Office, Center or Group Director approval prior to travel.

If approved, the traveler must contact the CMS International Team no less than 10 business days prior to departure to ensure the request is processed.

Note: All travelers will need to read and acknowledge receipt of the Foreign Travel Security Awareness Memorandum.

Questions? Please visit CMSnet, or contact the CMS International Team.

Protecting Information 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.

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

- *Rules of Behavior for Use of HHS Information Technology Resources*
- *HHS Policy for Personal Use of Information Technology Resources*
- *CMS Policy for the Acceptable Use of CMS Desktop/Laptop and Other IT Resources*

Topic 6: CMS Safeguards

- ✓ **Objective:** Recognize safeguards put in place to support information security and privacy protection.

Protect Your Identity

Protect Your Professional, and Personal, On-line Identity

- Hackers are known to gather information from accessible sources.
- Information about you on trade association and social media sites, professional ties and blogs all have the potential to help adversaries.
- This information is assembled and used to gain your trust in social engineering attacks.

Evaluate your on-line identity. How much can be learned about you?

Tips To Protect Your Identity

- Create strong passwords, do not reuse and manage them carefully
- Keep antivirus and other software up-to-date
- Validate emails before opening, check the email address, look for spelling errors, and check links
- Do not divulge personal information on social media
- Update privacy settings to only allow friends and family to see your posts.
- Check your credit report periodically

Knowledge Check

Check your Understanding

Let's review the information covered in this module with a few questions.

- These questions are for review only and will not be graded.
- Feedback will be provided for each question.
- Select **Next** when you are ready to begin.

Knowledge Check

Question 1

Social engineering attacks are more common and more successful than computer hacking attacks against the network.

A. True
B. False

Knowledge Check

Question1 Answer

Social engineering attacks are more common and more successful than computer hacking attacks against the network.

A. True
B. False

Social engineering attacks, including phishing attacks, malware and watering holes are more successful and common today than computer hacks. Use caution when visiting websites or opening new emails.

Knowledge Check

Question 2

When traveling or telecommuting it is okay to use the free Wi-Fi provided in cafés, airports and hotels.

A. True
B. False

Knowledge Check

Question 2 Answer

When traveling or telecommuting it is okay to use the free Wi-Fi provided in cafés, airports and hotels.

A. True
B. False

Malicious actors could be lurking in free Wi-Fi networks, 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).

Incidents: Impact and Response

Target: Healthcare Sector

Medical information is more valuable than credit card data to criminal hackers.*

- It cannot be replaced
- Access may be life/death
- Key to identify theft & a financial fraud tool

* Georgia Tech Institute for Information Security & Privacy 2017 Emerging Cyber Threats, Trends & Technology Report - http://www.iisp.gatech.edu/sites/default/files/documents/2017_threats_report_finalblu-web.pdf

Topic 1: Impact of an Incident or Breach

✓ **Objective:** Recognize the potential impact of a privacy or information system breach.

A Breach of Privacy

A Breach of Privacy is defined as:

"The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose."

OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

Repercussions of a Breach or Incident

A privacy and/or data breach can have serious repercussions for CMS, including:

- The inability for CMS to fulfill its mission.
- Disruption of day-to-day operations.
- Damage to the reputation of CMS.
- Harm to an individual's health or financial status.

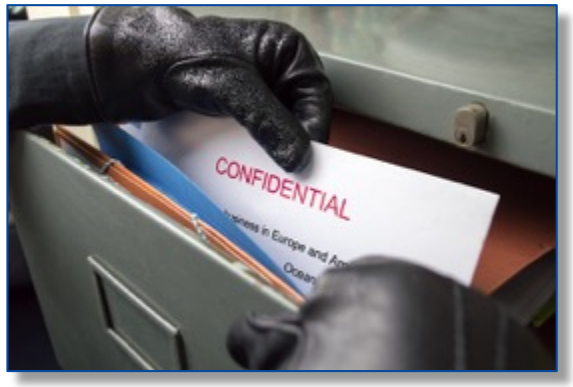
A breach or violations can result in severe consequences for the individuals involved, including employee discipline, fines and potentially imprisonment.

Know what to look for and how to prevent incidents or breaches from happening in the first place.

Types of Breaches or Incidents

A breach or incident may include:

- The intentional or unintentional release of PII or PHI without appropriate consent of the subject.
- The loss or theft of a government issued laptop, desktop, cell phone, smart phone, USB drive, or any portable device.
- The loss or unauthorized use of PII, PHI, Privacy Act or Sensitive Information.



Topic 2: Common Incidents & How To Respond

- ✓ **Objective:** Identify common types of security breaches or incidents.
- ✓ **Objective:** Identify the correct way to respond to a suspected or confirmed security or privacy incident.

Common Incidents

In the event of personal data being lost, stolen or misused, it is important to recognize how to respond. **A prompt and correct response could limit the severity of the breach and protect the privacy of individuals.**

Common incident scenarios that should be reported include:

- Physical Asset Disposal
- Misuse of ID numbers - SSN or MBI
- Spillage
- Sharing personal user credentials
- Unauthorized data
- Social engineering attacks

Physical Asset Disposal

- The loss, damage, theft, or improper disposal of equipment, media, or papers containing PII can lead to this information ending up in the wrong hands, resulting in an unauthorized disclosure.

SSNs and MBIs (Medicare Beneficiary Identifier)

The misuse of SSNs and MBIs puts individuals at risk for identity theft. Common types of misuse include:

- Using SSN or MBI's when not required or necessary.
- Using the full number instead of truncating or masking the number in systems or on paper printouts.
- Disclosing SSN or MBI's to those that do not have a need-to-know and are not authorized to receive the information.

Spillage

The Improper storage, transmission or processing of PII, PHI or any other Sensitive Information (SI).

Examples include:

- Unnecessarily sharing personal information with a person not authorized to view it.
- Storing personal information on unencrypted devices.
- Sending unencrypted emails.
- Faxing without first confirming you have the correct fax number and/or without calling the recipient afterwards to confirm receipt.

Sharing Credentials

- Allowing an unauthorized person to use your computer or credentials to access PII, PHI or SI.

Unauthorized Data

- Generating, receiving or sharing data not related to your authorized workflow

Social Engineering Attacks

- Any security situation that could compromise PII or PHI (e.g., virus, worm, ransomware, phishing email, social engineering attack.)

Responding to an Information Security or Privacy Incident

Report incidents to the CMS IT Service Desk:

- *1-800-562-1963 or 410-786-2580*
- *cms_it_service_desk@cms.hhs.gov*

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

Knowledge Check

Check your Understanding

Let's review the information covered in this module with a few questions.

- These questions are for review only and will not be graded.
- Feedback will be provided for each question.
- Select **Next** when you are ready to begin.

Knowledge Check

Question 1

A security breach or incident is defined as the intentional release of PII without the appropriate consent of the subject.

A. True

B. False

Knowledge Check

Question 1 Answer

A security breach or incident is defined as the intentional release of PII without the appropriate consent of the subject.

A. True

B. False

A security breach or incident is defined as the intentional or unintentional release of PII without the appropriate consent of the subject. It also encompasses the loss or theft of a government issued device or the loss or unauthorized use of PII, PHI, or SI.

Knowledge Check

Question 2

Amy left her laptop in a taxi cab on the way to the airport. What should she do? (Select 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.

Knowledge Check

Question 2 Answer

Amy left her laptop in a taxi cab on the way to the airport. What should she do? (Select 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.

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

HHS Rules of Behavior

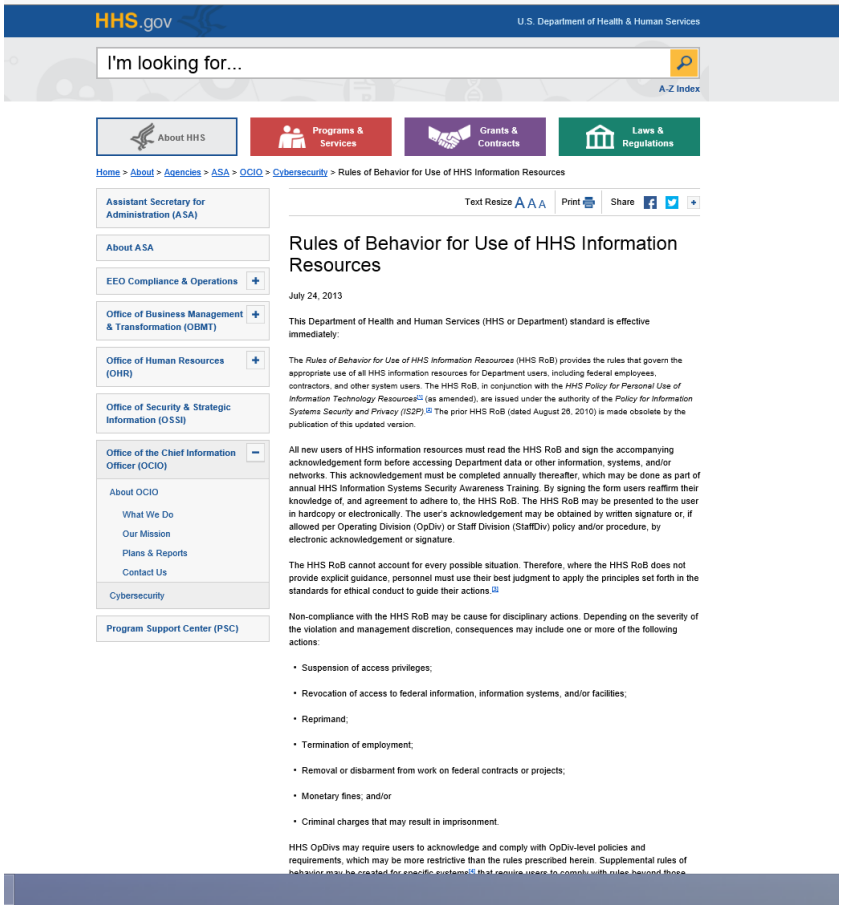
- **Objective:** Recognize your role in a successful information system security and privacy program.

HHS Rules of Behavior

A successful information security and privacy program begins with you.

The HHS Rules of Behavior govern the appropriate use of all HHS information resources and include:

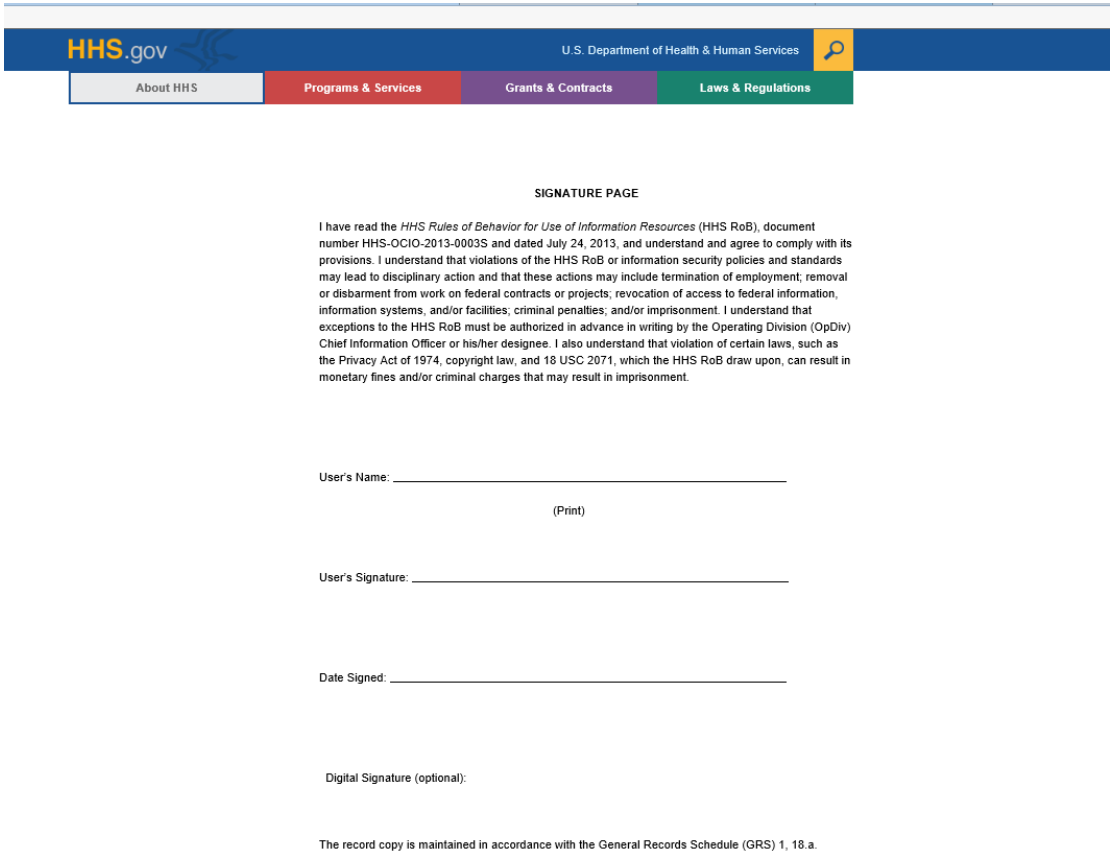
- General security and privacy practices
- Guidelines for handling sensitive information
- Your role in adhering to the Rules of Behavior
- Consequences for violations of the Rules



HHS Rules of Behavior and Acknowledgement

To successfully complete this course you will need to stop, read and **SIGN** the *HHS Rules of Behavior*.

- Print the HHS Rules of Behavior
- Read it thoroughly and sign it
- Provide a copy to your supervisor for future reference
- Maintain a copy for your records



For More Information

For all information systems security and privacy-related questions, contact the **CMS IT Service Desk** at:

Phone:

- 1-800-562-1963, or
  410-786-**2580**

Email:

- cms_it_service_desk@cms.hhs.gov

Dial straight down the line!