OFFICE OF THE
CHIEF INFORMATION OFFICER
DEPARTMENT OF HEALTH AND HUMAN SERVICES

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

The Department of Health and Human Services Cybersecurity Awareness Training

FISCAL YEAR 2016

Course Outline

- Course Introduction
- Lesson 1: Information Security Overview
- Lesson 2: Information Security Policy & Governance
- Lesson 3: Physical Access Controls
- Lesson 4: Email & Internet Security
- Lesson 5: Security Outside the Office
- Lesson 6: Privacy
- Lesson 7: Insider Threat
- Lesson 8: Incident Reporting
- Summary
- Rules of Behavior

COURSE INTRODUCTION

Cybersecurity Awareness Course

Welcome!

This course is designed to provide Department of Health and Human Services (HHS) employees, contractors, and others with access to Department systems and networks with the 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 awareness training for users of federal information systems.

When you are ready to continue, scroll down or use the right-arrow key on your keyboard.

HHS Mission

HHS employees and contractors enhance the health and well-being of Americans by providing for effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services.

Course Objectives

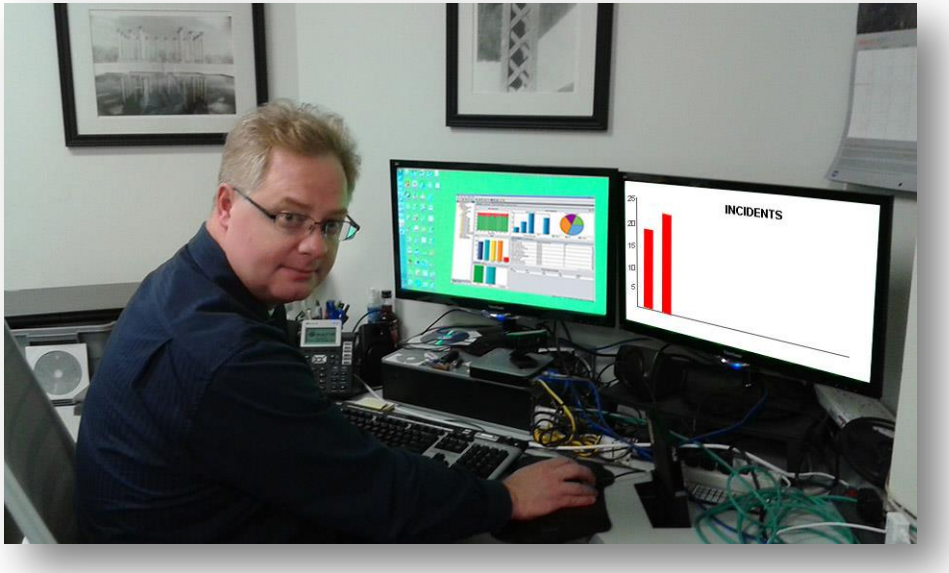
At the end of this course, you will be able to:

- Define information systems security;
- Identify federal regulations that mandate the protection of IT assets and information;
- Describe HHS' IT security and privacy policies, procedures, and practices;
- Define sensitive data;
- Describe your personal responsibility to protect information systems and privacy, and the consequences for violations;
- Recognize threats to information systems and privacy;
- Identify best practices to secure IT assets and data at the office or at home;
- Define privacy and personally identifiable information (PII);
- Define encryption and determine how and when to encrypt;
- Protect PII in different contexts and formats;
- List the traits that may indicate an insider threat; and
- Identify the correct procedure to report a suspected or confirmed security or privacy incident.

Course Information

Hi, I’m Mark Payne, your Information System Security Officer (ISSO) for this course. Throughout this course, you’ll help me to defend the Department’s information systems and information from hackers and cyber criminals.

Each of the lessons in this course covers an important aspect of cybersecurity awareness and privacy. Every so often, I’ll check back in with you and see how you’re progressing.



ISSO – Mark Payne

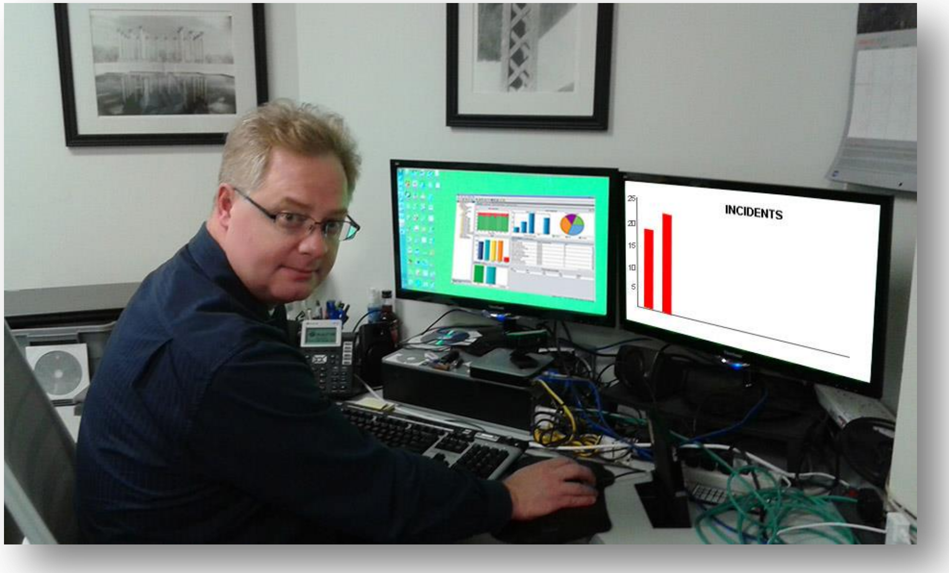
LESSON 1:
INFORMATION SECURITY OVERVIEW

Information Security

Hi, Mark again. Okay, so what is Information Security (INFOSEC)?

INFOSEC is how we protect 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 controls designed to protect the confidentiality, integrity and availability of information.
- The goal of an INFOSEC program is to understand, manage, and reduce the risk to information under the control of the organization.



ISSO – Mark Payne

Key Concepts

There are three elements to protecting information:

Confidentiality: Protecting information from unauthorized disclosure to people or processes.

Availability: Defending information systems and resources from malicious and unauthorized users to ensure accessibility by authorized users.

Integrity: Assuring the reliability and accuracy of information and IT resources.

Your bank ATM is a good example of a secure information system. You expect your bank ATM system to have confidentiality, availability, and integrity.

The amount of money in your account and your ATM personal ID number (PIN) should be **confidential**.

You expect that your account balance information and cash should always be **available** from the ATM machine.

The account balance information displayed by the ATM machine, and the amount of money dispensed by the machine must be accurate. In other words, have **integrity**.

.

Threats & Vulnerabilities

Threats and vulnerabilities put information assets at risk.

Threats are the potential to cause unauthorized disclosure, change, or destruction to an asset.

- Impact: potential breach in confidentiality, integrity failure and unavailability of information
- Types: natural, environmental, man-made

Vulnerabilities include any flaw or weakness that can be exploited and could result in a breach or a violation of a system’s security policy.

Risk is the likelihood that a threat will exploit a vulnerability.

Security Controls

IT security professionals use a combination of management, operational, and technical controls to manage risk:

Management: Accreditation is a management control as is having a System Security Plan.

Operational: Security awareness and training are operational controls as are physical security like guards, locks, and ID badges.

Technical: User ID and authentication (i.e. passwords) and access control lists are examples of technical controls.

What is Sensitive Data?

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

Examples of sensitive information include, but are not limited to:

- **Personally Identifiable Information (PII),**
- **Protected Health Information (PHI),**
- **Intellection Property, and**
- **Financial Data**

All sensitive information, including information stored or archived in shared folders, shall be available to authorized users only. Roles and responsibilities must be established and systems folders must be configured to allow least privileged access.

When safeguarding sensitive information, be sure to:

- Back up all stored or transmitted information, encrypt them, and file/archive the encrypted backup information.

Knowledge Check

What do you think is the goal of information security?

a) Protect identity, availability, and accuracy

b) Protect confidentiality, availability, and integrity

c) Protect availability, integrity, and accuracy

d) Eliminate threats, ensure integrity, and provide access

Knowledge Check Answer

What do you think is the goal of information security?

a) Protect identity, availability, and accuracy

b) Protect confidentiality, availability, and integrity

c) Protect availability, integrity, and accuracy

d) Eliminate threats, ensure integrity, and provide access

The correct answer is B!

The goal of information security is protecting confidentiality, availability, and integrity.

LESSON 2:
INFORMATION SECURITY POLICY & GOVERNANCE

Federal & Departmental Guidance

There are Federal and Departmental Guidelines that provide the backbone of IT security and privacy. Let’s take a look at the Federal Guidelines first.

IT Security Legislation and Guidance	Privacy Legislation	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) ‣ OMB-07-16	‣ NIST issues standards and guidelines to assist federal agencies in implementing security and privacy regulations. ‣ Special publications can be found at: NIST Publications.

Departmental Guidance

The **Department** sets programmatic direction by providing an enterprise-wide perspective, coordinating among key stakeholders, setting standards and providing guidance, and supporting streamlined reporting and metrics capabilities.

HHS Cybersecurity Program is the Department's information security program. Oversight is provided by the Office of the Chief Information Officer (CIO) and Chief Information Security Officer (CISO).

Operating Divisions (OpDivs) implement 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.

HHS-OCIO Policy for Information Systems Security and Privacy - Provides direction on developing, managing, and operating an IT security program to the OpDivs and Staff Divisions (StaffDivs).

HHS-OCIO Policy for Responding to Breaches of Personally Identifiable Information - Establishes actions taken to identify, manage, and respond to suspected or confirmed incidents involving Personally Identifiable Information (PII).

Rules of Behavior for Use of HHS Information Resources – Provides the rules that govern appropriate use of Department information resources. 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.

Knowledge Check

Who provides oversight for the Department's information security program?

a) Chief Financial Officer (CFO)

b) OpDiv Chief Information Security Officer (CISO)

c) Office of General Counsel (OGC)

d) Chief Information Officer (CIO)

Knowledge Check Answer

The correct answer is D!

Who provides oversight for the Department's information security program?

a) Chief Financial Officer (CFO)

b) OpDiv Chief Information Security Officer (CISO)

c) Office of General Counsel (OGC)

d) Chief Information Officer (CIO)

The CIO along with the Department (not OpDiv) CISO provides oversight.

Where to Get Guidance

It's important to be familiar with the Federal and Departmental Guidelines that inform the day-to-day information and information systems security rules and practices throughout the Department.

These documents are available to you from a variety of sources, including:

- Your Information Systems Security Officer (ISSO),
- Your OpDiv's Cybersecurity webpage, and
- The HHS Office of Information Security (OIS) policy website Home page at: http://intranet.hhs.gov/it/cybersecurity/policies/index.html

LESSON 3:
PHYSICAL ACCESS CONTROLS

Password Protection

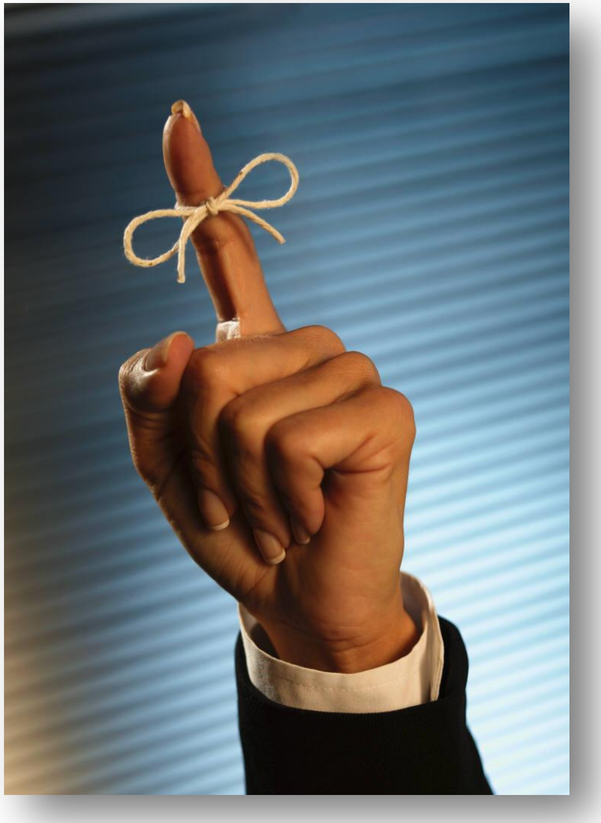
Your user identification (ID) along with a strong password is a deterrent to prohibit unauthorized users or processes from accessing your computer system.

While it is tempting to create an easy or generic password that is easy to remember, it is not very secure.

- Strong passwords have the following characteristics:
  - Eight or more characters in length
  - Characters from each of the following four categories:
    - Capital letter(s)
    - Lowercase letter(s)
    - Number(s)
    - Special character(s) (%,^,*,?,<,>)

Password Protection (continued)

- 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 ballgame!” becomes “Tmo2tBG!”
- Commit passwords to memory. If you are still having trouble, then write it down and keep it in a secure place, like your wallet.
- **DO NOT** keep passwords near your computer or on your desk.



Password Protection Tips

Here are some more important tips for protecting your password!

- **NEVER share your password with anyone.**
- Change your password every 60 days in accordance with HHS policy.
- Commit passwords to memory. If you’re still having trouble, then write it down and keep it in a secure place, like your wallet.
- Use a passphrase or mnemonic, like the initials to your favorite song, to help you remember your password.
- Change your password immediately if you suspect it’s compromised.
- Create a different password for each system or application.
- 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.

Knowledge Check

Which of the following is a strong password?

a) Timmy10

b) 123AbcTimmy4

c) T&E34dt72$R9k

d) Mustang_88!

Knowledge Check Answer

Which of the following is a strong password?

a) Timmy10

b) 123AbcTimmy4

c) T&E34dt72$R9k

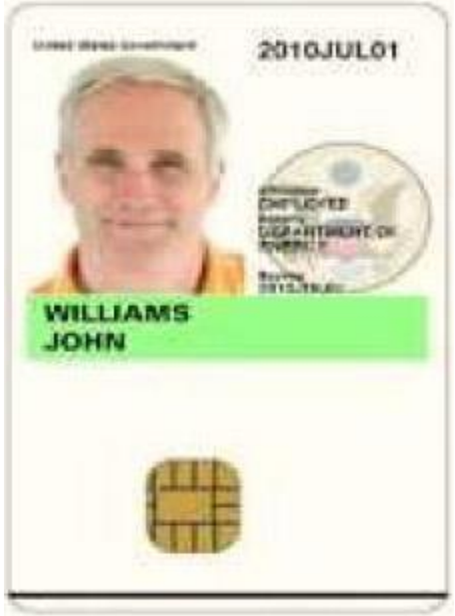
d) Mustang_88!

The correct answer is C!

Because it contains upper and lower case letters, numbers, and special characters (&!#$...).

Personal Identity Verification (PIV) Cards

In accordance with Homeland Security Presidential Directive 12 (HSPD-12), the Personal Identity Verification (PIV) Card shall be the primary Access Card used to facilitate physical access to HHS facilities, enable strong authentication for access to HHS networks, information systems, and information, as well as secure information while at rest and in transit by allowing for encryption, digital signatures and providing a higher level of assurance.



Personal Identity Verification (PIV) cards use smartchips that contain personally identifiable information (PII) and biometrics to reliably identify HHS staff. Because your PIV card grants you access to HHS facilities and (together with your PIN) to HHS computer networks and applications, you must maintain possession of it at all times. PIV cards are used to encrypt emails that contain PII and sensitive data.

The Federal Information Processing Standards (FIPS) Publication 201-2; Personal Identity Verification (PIV) of Federal Employees and Contractors standardizes the process for issuing ID badges throughout the federal government.

PIV Card Protection Tips

As a PIV card holder you are required to adhere to the following guidelines in order to safeguard and maintain your PIV card and credentials and ensure your associated record is kept up-to-date.

- Always remove your PIV card from your computer's card reader when leaving your desk.
- Memorize your PIN; *never* write it down.
- Keep it in a secure badge holder to shield it against unauthorized reading.
- Take all required actions to maintain your PIV credentials, i.e., timely renewal of your PIV certificates or PIV card upon receiving notice.
- Complete all mandatory training.

PIV Card Issues

Ensure you or your federal supervisor or organization notifies your badging office *immediately* if/when:

- You transfer to another organization within HHS,
- You leave HHS,
- Any of your personal information needs to be updated (e.g., name change or significant change in physical appearance),
- Your badge was lost, stolen or damaged and you need a replacement,
- Your badge no longer works after you attempted to update your certificate, or
- Your badge became locked after ten failed PIN entries.

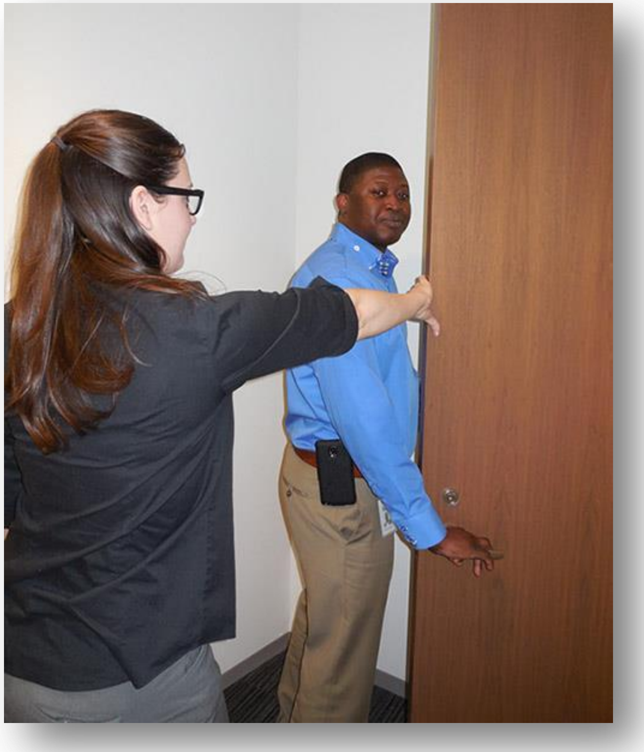
Return your PIV card to your federal supervisor, designated administrative contact, or badging office if/when you leave HHS.

Physical Security: Tailgating

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

Combat tailgating

- Employees must use their own badge to enter security doors. Never allow anyone to follow you into a 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 Security Tips

Here are some additional tips regarding physical security!

- **Only connect government authorized removable media devices. Do not use personal external hard drives or thumb drives on government equipment.**
- **Lock your computer when it's not in use (CTL + ALT + DELETE).**
- Encrypt all devices which contain PII and sensitive information.
- Store and transport removable media such as CDs, DVDs, flash drives, and external hard drives in a secure manner to prevent theft or loss.
- Don't leave sensitive information in plain sight when visitors are present or upon leaving your work area. Keep sensitive information in a secure safe or locked in a desk drawer.
- Quickly retrieve faxes that are sent to you. Always confirm that the recipient received the fax that you sent.

LESSON 4:
EMAIL & INTERNET SECURITY

Cyber Crime

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,
- Phishing, and
- Identity Theft.

Government information and information systems 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.

Social Engineering

These individuals may look trustworthy, but may be sophisticated cyber criminals.

They use social engineering techniques to obtain your personal information, access sensitive government information, and even steal your identity.

Social engineering is typically 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.

Social Engineering (continued)

Social engineering attacks are based on natural human desires like:

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

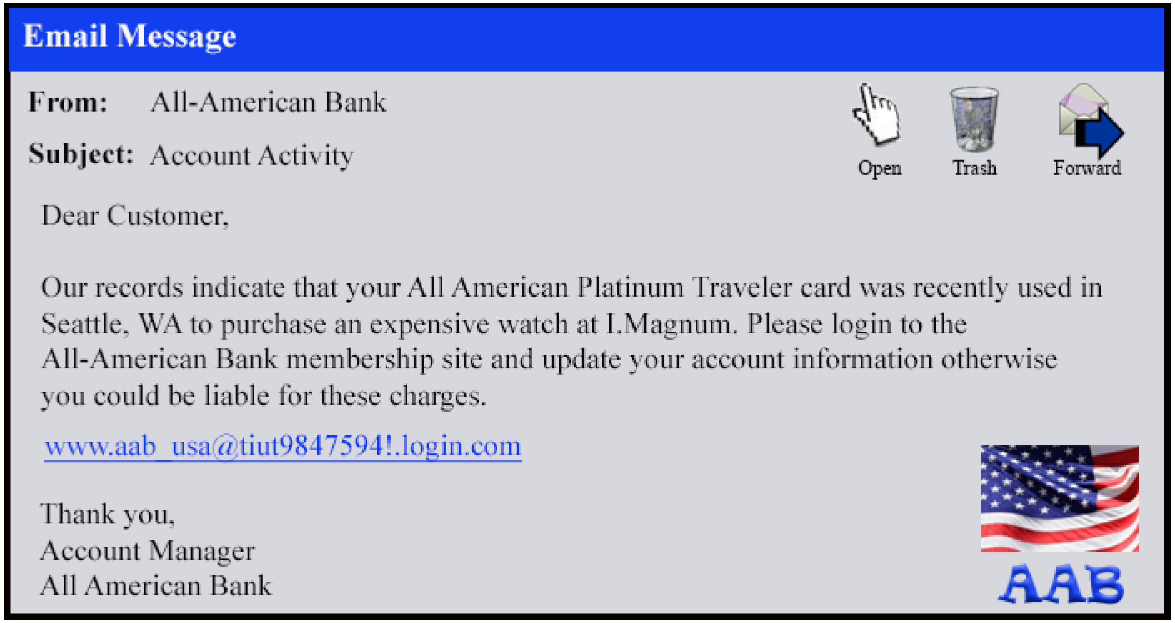
Common targets are:

- Passwords,
- Security badges,
- Access to secure areas of the building,
- Uniforms,
- Smart phones,
- Wallets, and
- Employee’s personal information.

Phishing Attacks

Phishing is a social engineering scam whereby intruders seek access to your personal information or passwords 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 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 authentic web address. For example "Amazons.com". Here is an example:



Email Message

From: All-American Bank

Subject: Account Activity

Dear Customer,

Our records indicate that your All American Platinum Traveler card was recently used in Seattle, WA to purchase an expensive watch at I.Magnum. Please login to the All-American Bank membership site and update your account information otherwise you could be liable for these charges.

www.aab_usa@tiut9847594!.login.com

Thank you,
Account Manager
All American Bank

Phishing Attacks (continued)

Two types of phishing you need to be aware of are:

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.

NEVER provide your password to anyone via email. Be suspicious of any email that:

- Requests personally identifiable information (PII),
- Contains spelling and grammatical errors,
- Asks you to click on a link,
- Is unexpected or from a company or organization with whom you do not have a relationship, or
- Has a different uniform resource locator (URL) web address than the one you typically use.

Avoid the Bait

Here are some more important tips for protecting yourself from Phishing Attacks!

If you are suspicious of an email:

- **Do** forward the email to spam@hhs.gov and then delete it from your Inbox.
- **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.

Identity Theft

Let’s talk about why “phishers” do what they do. One major reason that impacts you directly is 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.

Identity Theft (continued)

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.

Identity Theft (continued 2)

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, address, account numbers, and PII.

Malware

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

Email links and attachments are two of the most common sources of malware infection.

Some examples of malware are:

- Viruses, Worms, Trojan Horses, Root Kits, and Spyware.

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 your HHS Computer Security Incident Response Center (CSIRC) by email at csirc@hhs.gov or phone 866-646-7514; or contact your security POC.

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.

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 spam@hhs.gov or the security POC for your office.

What is Encryption?

Encryption is the conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

It's important to encrypt files containing PII. Please be sure to refer to your individual helpdesk for instructions on how to use encryption technology.

Personal Identity Verification (PIV) and Public Key Infrastructure (PKI) cards are the first choice for encryption.

Encryption Alternatives can be found by visiting: http://intranet.hhs.gov/it/cybersecurity/enterprise_security/Encryption/

Appropriate Use of Email

HHS email accounts are for official business. Personal email should NEVER be used to conduct official HHS government business.

- Review the *Rules of Behavior for Use of HHS Information Resources* for more information.
- **Emails that contain sensitive data must be encrypted before being sent.** Information on encryption solutions can be found at:

  http://intranet.hhs.gov/it/cybersecurity/enterprise_security/Encryption/index.html

Employees are permitted limited personal use of email. HHS email accounts must not be used 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.

Personal emails should not:

- Disrupt employee productivity, disrupt service or cause congestion on the network (e.g., sending spam or large media files), or to engage in inappropriate activities.

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 OpDiv CIO. Speak to your manager for more information.

Cookies

A cookie is a text file that a website automatically puts on your hard drive that saves information that you type in like preferences or user name. Use cookies with caution.

- 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

- Confirm that websites requesting personal information are encrypted and the URL begins with “https”.
- There is risk anytime you enter personal information on a website.
- Set your browser Internet Options, Privacy settings to notify you when a website requests to install a cookie.
- Periodically delete all Cookies and website data from your browser history.

ActiveX

ActiveX is a form of mobile code technology that allows Internet browsers to run small applications online.

- Code has the capability to alter your operating system which can cause a software failure if the code is malicious.

<u>Protect your computer</u>

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

Knowledge Check

Complete this sentence: 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

Knowledge Check Answer

Complete this sentence: 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**

The correct answer is D!

Phishing is a type of social engineering. It often appears to be from an organization you know, and almost always has a link or an attachment.

LESSON 5:
SECURITY OUTSIDE THE OFFICE

Security Outside the Office

Don’t be the Breach!

Be vigilant about protecting HHS information and information systems when on travel or working at remote locations.

Security researchers say that 68% of data breaches at U.S. healthcare companies are caused by employees losing, or the theft of, laptops or other mobile devices[1].

It is your responsibility to protect HHS technology and resources that are assigned to you when you are outside of the office.

#DontBeTheBreach

[1] 2014 Bitglass Healthcare Breach Report

Travel & Remote Location Tips

Here are more important tips for protecting information systems while working outside the office!

- **Turn off your laptop while travelling so that encryption is enabled**.
- Always maintain possession of your laptop and other mobile devices.
- Ensure that the wireless security features are properly configured by using only approved secure Virtual Private Network (VPN) ports.
- 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 Local Area Network (LAN) cable.
- Report a loss or theft of your laptop or other government furnished device immediately to your security POC and Privacy representative.

Telework

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

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

Protect information and data while teleworking

- Always maintain possession of your laptop 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.

Protecting PII While Teleworking

There are special responsibilities for protecting PII during telework:

You must follow standard security procedures when removing official records from the office, and have permission from your manager to transport, transmit, remotely access or download sensitive or classified information during telework.[2]

HHS encryption is critical. It's extremely important to store sensitive information on authorized mobile devices or remote systems with appropriate safeguards.[3]

Remotely access sensitive information by using authorized methods (e.g., VPN).

[2] *HHS Telecommuting Program Policy*
[3] *HHS-OCIO Policy for information Systems Security and Privacy (IS2P)*

Home Security

Safeguarding your computer at home is important! Ensure that you do the following:

- 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 and encrypt your files.
- Follow the instructions in the user manual to enable encryption for your wireless router.
- Use encryption software to send encrypted sensitive and PII data on your home computer.
- Install and update the latest operating system (OS) security patches.

Knowledge Check

Which of the following must you do when travelling or teleworking?

a. Lock up any files or documents containing PII
b. Keep possession of your laptop at all times
c. Turn off/disable wireless capability when connected via LAN cable
d. Report the loss or theft of any government furnished device immediately to security and Privacy representatives
e. All of the above

Knowledge Check Answer

Which of the following must you do when travelling or teleworking?

a. Lock up any files or documents containing PII

b. Keep possession of your laptop at all times

c. Turn off/disable wireless capability when connected via LAN cable

d. Report the loss or theft of any government furnished device immediately to security and Privacy representatives

e. All of the above

You got it! You have to do all of these.

The correct answer is E!

LESSON 6:

PRIVACY

What is Privacy?

Personal Privacy is the right to be free from physical intrusion to one's personal space or solitude. It allows individuals a choice in how their personally identifiable information (PII) is used and disclosed.

Information Privacy is a set of fair information practices that ensure personal information is accurate, relevant, and current. Additionally, Information Privacy promotes trust between HHS and the American public by:

- Protecting individuals' personal information,
- Using personal information appropriately, and
- Assuring that personal data is used and viewed only for business purposes.

Why is Privacy Important?

As a member of the HHS workforce, each of us is responsible for protecting privacy. Privacy is important because it allows us to earn and keep public trust, prevent identity theft, prevent privacy incidents, and follow the law. Privacy policy and procedures require that we:

- Collect, access, use, and disclose personal information only for reasons that are for a legitimate job function, support the mission of HHS, and are allowed by law.
- Safeguard personal information in your possession, whether it be in paper or electronic format.
- Properly dispose of documents containing PII. Shred papers; NEVER place them in the trash.
- Contact the IT Department for proper disposal of equipment like copy machines, printers and computers[1].
- Report suspected privacy violations or incidents[2].

1. These devices contain memory that can retain PII long after you've used the device.
2. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

Consequences of Privacy Violations

Privacy violations have several possible consequences, which include:

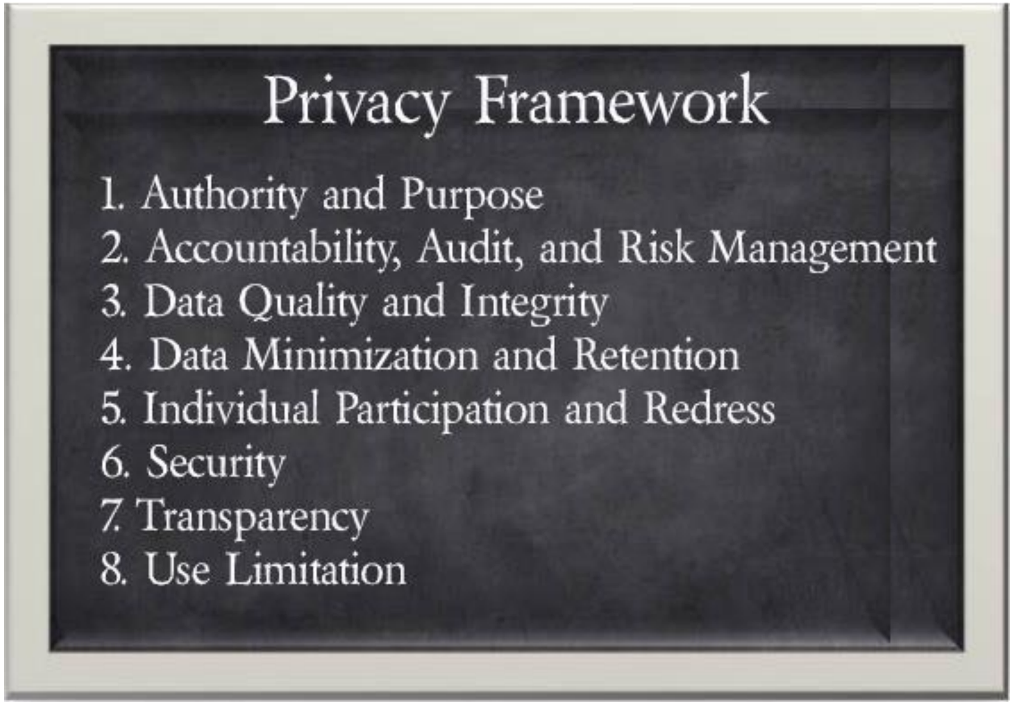
Employee discipline

Fines

Imprisonment

Fair Information Practice Principles

HHS has long been a major force in establishing and meeting high standards for privacy. In 1973, HHS[3] advanced the Code of Fair Information Practice which has served as a foundation for future federal privacy frameworks. Shown here is an example of one of the many frameworks developed to encompass and expand HHS' early framework:



Privacy Framework

1. Authority and Purpose
2. Accountability, Audit, and Risk Management
3. Data Quality and Integrity
4. Data Minimization and Retention
5. Individual Participation and Redress
6. Security
7. Transparency
8. Use Limitation

[3] Formerly known as the Department of Health Education and Welfare (HEW)

What is PII?

Personally Identifiable Information (PII) is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

These are some examples of PII:

- Name,
- Social Security number (SSN),
- Date of birth (DOB),
- Mother’s maiden name,
- Financial records,
- Email address,
- Driver’s license number,
- Passport number, and
- Personal Health information (PHI).

Putting Privacy Into Action

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

Here are the first four principles in more detail.

Framework	Description	Examples
Authority and Purpose	HHS publically documents the purpose for which the PII is collected at the time of the 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
Accountability, Audit, and Risk Management	Individuals have a clear understanding of their responsibilities for handling PII. Systems owners and program managers understanding are accountable for understanding the risks and responsibilities of handling PII in their systems and programs and report these appropriately.	• Privacy Impact Assessments • Privacy training and awareness
Data Quality and Integrity	HHS 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).
Data Minimization and Retention	HHS 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

Putting Privacy Into Action (continued)

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

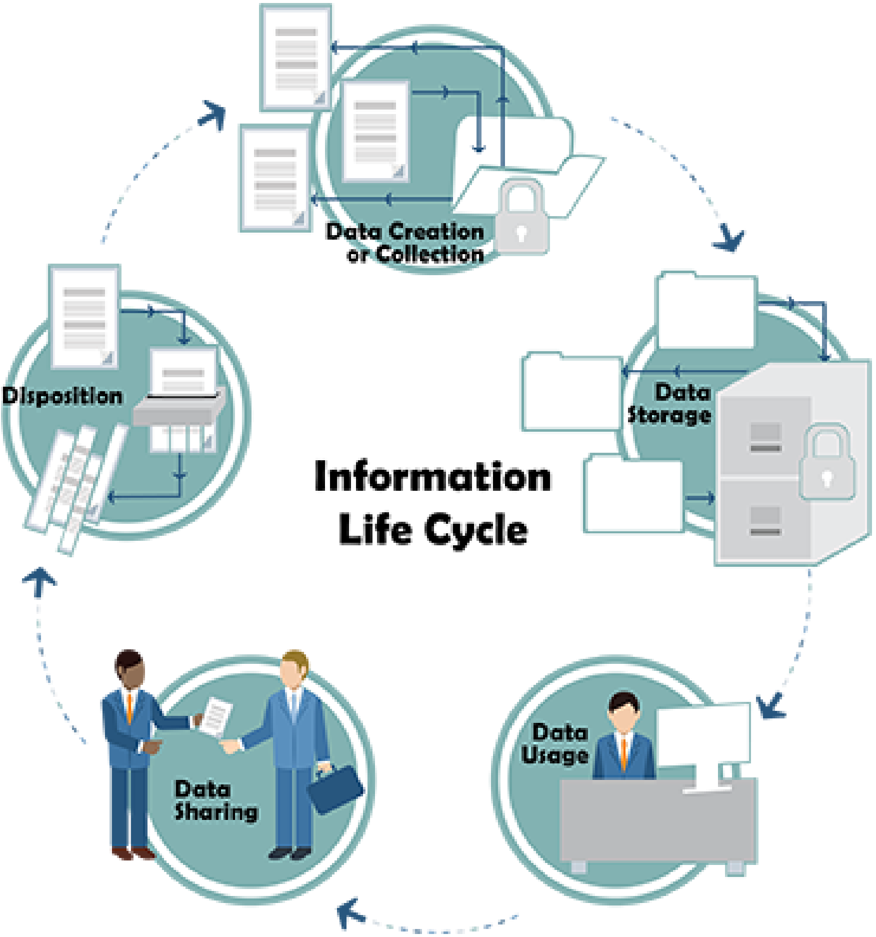
Here are the last four principles in more detail

Framework	Description	Examples
Individual Participation and Redress	Individuals provide HHS 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 of Record • Individuals can request that errors be corrected (redress)
Security	HHS protects PII, in all formats, through administrative, technical, and physical security safeguards with guard against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.	• Encryption • Shredding • User Names and passwords • Locks
Transparency	HHS provides a notice to individuals regarding the collection, use, dissemination, and maintenance of PII.	• Privacy Act Statements • Privacy policy on websites • System of Records Notices in Federal Register
Use Limitation	HHS 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 with 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

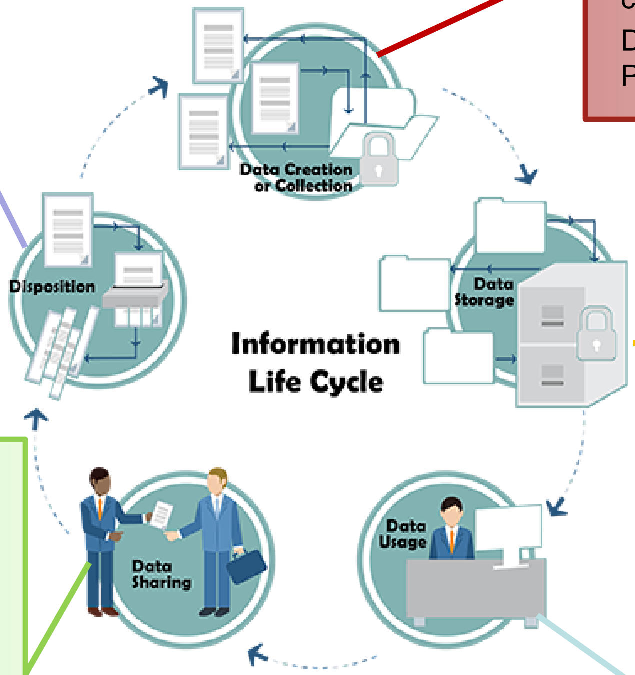
PII Considerations for the Information Life Cycle

The HHS Information Life Cycle defines how to handle and encrypt data from inception to disposition. Protecting PII is **required** during each stage of the cycle:

- **Data Collection or Creation:** Gathering PII for use.
- **Data Storage:** Maintaining or storing PII. When safeguarding sensitive information, back up all stored or transmitted information, encrypt them, and file/archive the encrypted backup information.
- **Data Usage:** Using PII to accomplish a job function.
- **Data Sharing:** Disclosing or transferring PII.
- **Disposition:** Disposing of PII in accordance with record management requirements and organizational disposal policies.



PII Considerations for the Information Life Cycle (cont’d)



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?

Did you follow proper encryption security procedures to secure the stored PII?

Did you secure documents and files that contain PII?

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

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?

Were the appropriate encryption safeguards put in place prior to sharing?

Did you send PII to only secure email addresses?

Did you verify that the sharing is allowed?

Have you verified that everyone receiving the PII has a need to know?

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

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?

Protecting PII While in Transit

You must protect PII during transit. Please **remember**:

- **To** encrypt emails that contain PII. **All HHS information systems that store or process sensitive information must protect the confidentiality and integrity of data at rest and data in transit by employing cryptographic mechanisms in accordance with HHS policies.**
- **DO NOT** forward work emails with PII to personal accounts (e.g., Yahoo, Gmail). Keep work and personal emails separate!
- **To avoid** interaction with unauthorized websites when PII is involved (e.g. Wikis).
- All HHS sensitive information **must be secured with FIPS 140-2 encryption solution while in transit**.
- Users should report all suspected computer security incidents to their local Operating Division (OpDiv) Computer Security (CSIRT)/ Incident Response Team (IRT) or Help Desk.

Protecting PII At Your Workstation

Maintain a clean work environment.

- Don’t leave documents that contain PII on your printer or at printer stations.
- Don’t leave files or documents containing PII unsecured on your desk when you are not there.
- Check your workstation before you leave at the end of the day.
- Lock your laptop or desktop (ctl+alt+del)

Protecting PII When Faxing

Sending faxes:

- Verify recipient's fax number prior to sending PII.
- Make sure someone authorized to receive the PII is there to receive the fax.
- Use a fax transmittal sheet.
- Don't leave PII on fax machines after faxing.

Receiving faxes:

- Quickly retrieve faxes transmitted to you.
- Secure faxes that have not been retrieved.
- If you are expecting a fax and have not received it, follow-up to ensure the sender has the correct fax number.

Protecting PII When Mailing

Interoffice mail:

- Send in a confidential envelope.
- Follow-up to verify that the recipient received the information.

Postal mail (“snail mail”):

- When possible, use a traceable delivery service (like UPS).
- Package in an opaque envelope or container.

Email:

- Double-check the recipient’s address before sending.
- Encrypt email.
- Digitally sign email.

Protecting PII with Encryption

Always encrypt internal and external emails that contain PII.

- **Personal identity verification (PIV) and public key infrastructure (PKI) cards are the first choice for encryption.**
- When that is not possible, visit http://intranet.hhs.gov/it/cybersecurity/enterprise_security/Encryption/ for **encryption alternatives.**

Encrypt files containing PII.

- Do not send the password via encrypted email.
- Provide the password either in person, over the phone or by text message.
- **Be sure to refer to your individual helpdesk for instructions on how to use encryption technology.**

SSN Protections

Employees who handle SSNs need to take extra precautions. Misuse of SSNs can put individuals at risk for identity theft.
Employees should:

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

Disposition

Tips for disposing of PII when it's no longer needed:

- Review records retention requirements prior to destroying information.
- Shred papers containing PII.
- Dispose of electronic devices by returning to the IT Department.

Knowledge Check

When emailing a file that contains PII which of the following should you do?

a. Only send information to email addresses certified to receive top secret documents
b. Hide your computer screen from anyone that may be watching you
c. Only email from home so no one can see what you are sending
d. Make sure that you've securely encrypted the email and have verified that everyone receiving the email has a need to know

Knowledge Check Answer

The correct answer is D!

When emailing a file that contains PII which of the following should you do?

a. Only send information to email addresses certified to receive top secret documents.

b. Hide your computer screen from anyone that may be watching you.

c. Only email from home so no one can see what you are sending.

d. Make sure that you've securely encrypted the email and verified that everyone receiving the email has a need to know.

Only verified recipients should receive the email with the PII. Email should be encrypted and only sent to secure (not personal) email addresses.

Privacy Points of Contact

For specific privacy-related questions, contact:

- OPDIV Senior Official for Privacy (SOP) http://intranet.hhs.gov/it/cybersecurity/privacy/index.html

- Privacy Act Contacts http://www.hhs.gov/foia/contacts/index.html#privacy

To learn more:

- Visit the HHS Cybersecurity Privacy page http://intranet.hhs.gov/it/cybersecurity/privacy/index.html for more information on protecting PII and incident response.

- Visit the HHS Cybersecurity Privacy Resource Center http://intranet.hhs.gov/it/cybersecurity/privacy/prc/index.html for tips on how to protect PII at work and at home.

LESSON 7:

INSIDER THREAT

Definition of an Insider Threat

What is an insider threat?

A malicious insider threat is a current or former employee, contractor, or other business partner who has or had authorized access to an organization’s network, system, or data and intentionally misused that access in a manner that negatively impacts the confidentiality, integrity, or availability of the information or information system.

This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of Departmental resources or capabilities (source: U.S. Computer Emergency Readiness Team (CERT)).

Why is HHS a Target?

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 including:

- U.S. and global public health policies and positions,
- Medical countermeasure research, development, and acquisition information,
- Senior expertise in exotic, infectious, and pandemic diseases,
- Information about innovative life science research data and best practices,
- State-of-the-art high-containment laboratories,
- The U.S. repository of proprietary food and drug-related information, and
- Public health and medical preparedness and response operations.

Threat Indicators

Although no single indicator provides conclusive proof or evidence that an individual is an insider threat, some suspicious behaviors could include:

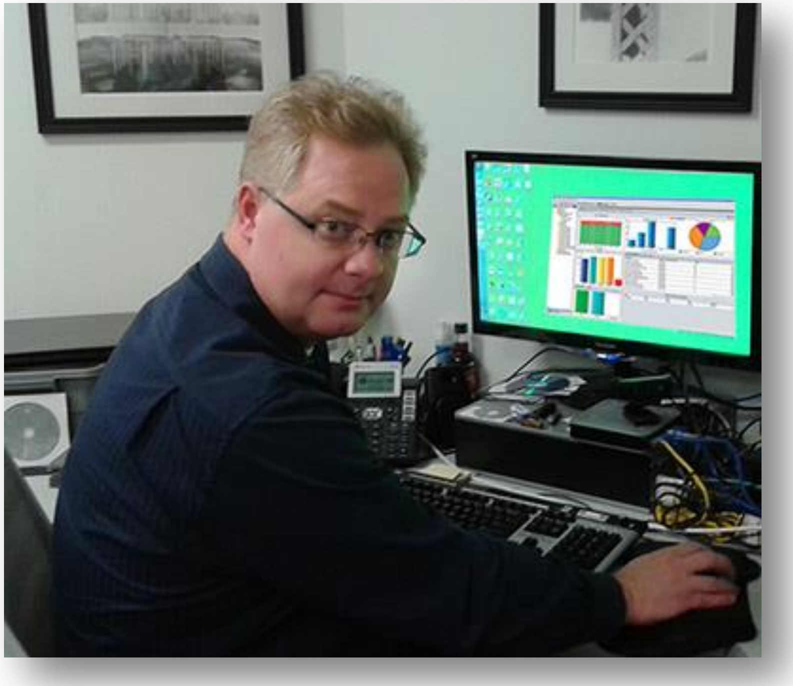
- Unreported contact with foreign nationals outside the scope of official business,
- Disclosed or removed sensitive, proprietary, or classified information without approval,
- Unexplained reproduction or transmission of classified or sensitive information,
- Attempted access to classified or sensitive information beyond scope of duties,
- Expressed support or action for international terrorist organizations or objectives,
- Expressed hatred of American society, culture, government, or principles of the U.S. Constitution,
- Contributed financially to a foreign charity, institutions, or individuals associated with terrorism, and
- Difficult life circumstances: alcohol, drugs, divorce, etc.

Be Aware

The most important tip is to be aware of what is going on around you with your coworkers.

If you notice a coworker who is:

- Having financial difficulties,
- Alcohol, drug, or mental health issues and not seeking treatment,
- Appearing to live beyond their means, or
- Aggressively trying to get access to information systems and data that they have no “need to know”.



Let someone know. Report the incident to: **Counterintelligence Directorate at awareness@hhs.gov**

LESSON 8:
INCIDENT REPORTING

Causes of Data & Privacy Incidents

If any of the following privacy and/or data incidents happen to you, please report it!

- Loss, damage, theft, or improper disposal of equipment, media, or papers containing PII.
- Accidentally sending PII in any form to a person not authorized to view the report or sending it unencrypted.
- Allowing an unauthorized person to use your computer or credentials to access PII.
- Discussing work related information, such as a person’s medical 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).

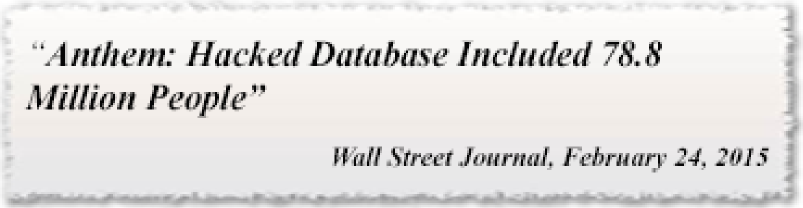
Consequences of Data & Privacy Incidents

Privacy and data incidents can result in:

- Inability for HHS to fulfill its mission, and
- Disruption of day-to-day operations.

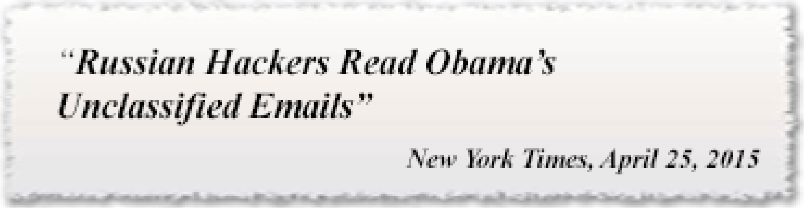
Additionally, loss of privacy threatens people and HHS. It can result in:

- Exploitation of an individual's health or financial status,
- Embarrassment or harm to individuals,
- Damage to the reputation of HHS, and
- Loss of trust between HHS and the public.



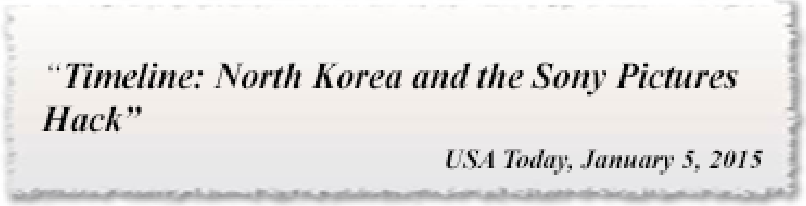
"Anthem: Hacked Database Included 78.8 Million People"

Wall Street Journal, February 24, 2015



"Russian Hackers Read Obama's Unclassified Emails"

New York Times, April 25, 2015



"Timeline: North Korea and the Sony Pictures Hack"

USA Today, January 5, 2015

How To Report

Within HHS, users should report all suspected computer security incidents to their local Operating Division (OpDiv) Computer Security (CSIRT)/ Incident Response Team (IRT) or Help Desk

http://intranet.hhs.gov/it/cybersecurity/docs/policies_guides/OCIO/pol-pers-use-it-rsrc.pdf

Contact information for each OpDiv can be found at: http://intranet.hhs.gov/it/cybersecurity/hhs_csirc/

Please see the chart below for each OPDIV CSIRT contact.

OpDiv	Email
ITO	Hhsitio-irt@hhs.gov
AHRQ	csirt@ahrq.hhs.gov
ACF	Gary.cochran@acf.hhs.gov
ACL	csirt@acl.hhs.gov
SAMHSA	infosecurity@samhsa.hhs.gov
CMS	soc@cms.hhs.gov
FDA	csirt@fda.hhs.gov
CDC/ATSDR	csirt@cdc.gov
IHS	irt@ihs.gov
NIH	csirt@nih.hhs.gov
OIG	csirt@oig.hhs.gov
HRSA	csirt@hrsa.hhs.gov

Reporting Incidents Tips

Important tips on reporting data and privacy incidents:

- Do not investigate the incident on your own - *immediately* report suspected incidents, especially those that could compromise PII, regardless of whether it's in electronic, paper, or oral format.
- 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.
- Agencies that share information on terrorism or counterintelligence are participating in what is known as the Information Sharing Environment (ISE). Prior to sharing information via the ISE, be sure you are aware of its specific privacy requirements. For questions about the ISE, contact the HHS Office of Security and Strategic Information (OSSI).

Reporting Insider Threats

Insider threats are a special type of incident. Report these incidents to the OSSI:

Counterintelligence Directorate at awareness@hhs.gov

Knowledge Check

Which of the following should you report?

a. Theft of your Department-issued Blackberry
b. A coworker breaking into a file cabinet that’s not theirs
c. Loss of some important documents containing research subject’s SSNs
d. Inadvertently clicking on a link in a Phishing email
e. All of the above

Knowledge Check Answer

The correct answer is E!

Which of the following should you report?

a. Theft of your Department-issued Blackberry
b. A coworker breaking into a file cabinet that's not theirs
c. Loss of some important documents containing research subject's SSNs
d. Inadvertently clicking on a link in a Phishing email
e. All of the above

All of these examples are reportable incidents.

SUMMARY:

Review of Objectives

In this course, you have learned to:

- Define information systems security;
- Locate federal regulations that mandate the protection of IT assets and information;
- Describe HHS' IT security and privacy policies, procedures, and practices;
- Define sensitive data;
- Describe your personal responsibility to protect information systems and privacy, and the consequences for violations;
- Recognize threats to information systems and privacy;
- Define encryption and determine how and when to encrypt;
- Perform HSS best practices to secure IT assets and data at the office or at home;
- Define privacy and personally identifiable information (PII);
- Define encryption and determine how and when to encrypt;
- Protect PII in different contexts and formats;
- Identify the traits that may indicate an insider threat; and
- Report a suspected or confirmed security or privacy incident to the proper authorities.

COURSE QUIZ:

Quiz Question 1 of 10

Read the following statement and determine if it’s True or False:

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

a. True

b. False

Quiz Question 1 of 10 Answer

Read the following statement and determine if it’s True or False:

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

a. True

b. False

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

Quiz Question 2 of 10

Who sets programmatic direction by providing an enterprise-wide perspective, facilitating coordination among key stakeholders, setting standards and providing guidance for the protection of information and information systems?

a. The Department (HHS)
b. Each OpDiv
c. Individual offices
d. Individual Information Systems Security Officers (ISSOs)

Quiz Question 2 of 10 Answer

Who sets programmatic direction by providing an enterprise-wide perspective, facilitating coordination among key stakeholders, setting standards and providing guidance for the protection of information and information systems?

a. The Department (HHS)

b. Each OpDiv

c. Individual offices

d. Individual Information Systems Security Officers (ISSOs)

The Department of Health and Human Services sets programmatic direction at the enterprise level.

Quiz Question 3 of 10

Which of the following represents a strong password?

a. JohnnyAppleseed
b. Wanda434
c. rdCamero$$
d. TGiF23$a4Vs@87

Quiz Question 3 of 10 Answer

Which of the following represents a strong password?

a. JohnnyAppleseed
b. Wanda434
c. rdCamero$$
d. TGiF23$a4Vs@87

Answer “d” uses a combination of upper case and lower case letters, numbers, and special characters. It’s also longer than 8 characters and not easy to guess.

Quiz Question 4 of 10

With regard to your PIV card you, or your federal supervisor or organization should notify your badging office immediately if which of the following occurs?

a. You leave the employ of HHS
b. You lose your PIV card
c. Any of your personal information has changed
d. Any of the above

Quiz Question 4 of 10 Answer

With regard to your PIV card you, or your federal supervisor or organization should notify your badging office immediately if which of the following occurs?

a. You leave the employ of HHS
b. You lose your PIV card
c. Any of your personal information has changed
d. Any of the above

Notify your badging office if any of these situations occur.

Quiz Question 5 of 10

An email might be a phishing email if…

a. It contains a lot of spelling and grammar errors
b. It appears to come from a legitimate organization, but not one you do business with online
c. Asks you to click on a link and provide personal information
d. Any of the above

Quiz Question 5 of 10 Answer

An email might be a phishing email if…

a. It contains a lot of spelling and grammar errors
b. It appears to come from a legitimate organization, but not one you do business with online
c. Asks you to click on a link and provide personal information
d. Any of the above

All of these indicators might be present in a phishing email. In general be aware of links or attachments in any email from anyone you were not expecting the request.

Quiz Question 6 of 10

Read the following statement and determine if it’s True or False:

Personal email accounts should NEVER be used to conduct official HHS government business.

a. True

b. False

Quiz Question 6 of 10 Answer

Read the following statement and determine if it’s True or False:

Personal email accounts should NEVER be used to conduct official HHS government business.

a. True

b. False

True, you should NEVER use your personal email accounts to conduct official HHS government business.

Quiz Question 7 of 10

The number one cause of data breaches at U.S. healthcare companies is:

a. Hackers finding a back-door into a system
b. An intruder tailgating through a secure door
c. An employee losing a laptop or Blackberry device
d. Employees discussing PII in elevators

Quiz Question 7 of 10 Answer

The number one cause of data breaches at U.S. healthcare companies is:

a. Hackers finding a back-door into a system
b. An intruder tailgating through a secure door
c. An employee losing a laptop or Blackberry device
d. Employees discussing PII in elevators

One study estimates that 68% of all data breaches are caused by employees losing equipment or data. Keep your laptop and other devices with you at all times.

Quiz Question 8 of 10

Protect information and data while teleworking by…

a. Only leaving your laptop with someone you work with
b. Reporting lost or stolen equipment immediately
c. Only using free Wi-Fi hotspots in hotel rooms and public area
d. Only using your personal laptop when teleworking

Quiz Question 8 of 10 Answer

Protect information and data while teleworking by…

a. Only leaving your laptop with someone you work with

b. Reporting lost or stolen equipment immediately

c. Only using free Wi-Fi hotspots in hotel rooms and public area

d. Only using your personal laptop when teleworking

Always report the loss or theft of a device immediately.

Quiz Question 9 of 10

HHS protecting PII, in all formats, using administrative, technical, and physical security safeguards, is a description of which of the eight Privacy Framework Principles?

a. Security

b. Data Minimization and Retention

c. Data Quality and Integrity

d. Transparency

Quiz Question 9 of 10 Answer

HHS protecting PII, in all formats, using administrative, technical, and physical security safeguards, is a description of which of the eight Privacy Framework Principles?

a. Security
b. Data Minimization and Retention
c. Data Quality and Integrity
d. Transparency

Protecting PII through the use of these controls best describes the Privacy Framework Principle #6: Security.

Quiz Question 10 of 10

An insider threat may:

a. Disclose or remove sensitive information without approval
b. Reproduce classified or sensitive information for no apparent reason
c. Express hatred of American society or government
d. Any of the above

Quiz Question 10 of 10 Answer

An insider threat may:

a. Disclose or remove sensitive information without approval

b. Reproduce classified or sensitive information for no apparent reason

c. Express hatred of American society or government

d. Any of the above

Insider threats may display any of these behaviors. They may also act disgruntled or angry quite often during the day.

Congratulations

You have completed the Cybersecurity Awareness Course!

Click Next to read and acknowledge the *HHS Rules of Behavior For Use of HHS Information Resources.*

HHS Rules of Behavior

Rules of Behavior for Use of HHS Information Resources
Office of the Chief Information Officer
Office of the Assistant Secretary for Administration
Department of Health and Human Services

July 24, 2013

This Department of Health and Human Services (HHS or Department) standard is effective immediately:

The *Rules of Behavior for Use of HHS Information Resources* (HHS RoB) provides the rules that govern the appropriate use of all HHS information resources for Department users, including federal employees, contractors, and other system users. The HHS RoB, in conjunction with the *HHS Policy for Personal Use of Information Technology Resources*[1] (as amended), are issued under the authority of the *Policy for Information Systems Security and Privacy (IS2P).*[2] The prior HHS RoB (dated August 26, 2010) is made obsolete by the publication of this updated version.

All new users of HHS information resources must read the HHS RoB and sign the accompanying acknowledgement form before accessing Department data or other information, systems, and/or networks. This acknowledgement must be completed annually thereafter, which may be done as part of annual HHS Information Systems Security Awareness Training. By signing the form users reaffirm their knowledge of, and agreement to adhere to, the HHS RoB. The HHS RoB may be presented to the user in hardcopy or electronically. The user's acknowledgement may be obtained by written signature or, if allowed per Operating Division (OpDiv) or Staff Division (StaffDiv) policy and/or procedure, by electronic acknowledgement or signature.

[1] Available at: http://www.hhs.gov/ocio/policy/index.html
[2] Available at: http://www.hhs.gov/ocio/policy/index.html

HHS Rules of Behavior 2

The HHS RoB cannot account for every possible situation. Therefore, where the HHS RoB does not provide explicit guidance, personnel must use their best judgment to apply the principles set forth in the standards for ethical conduct to guide their actions.

Non-compliance with the HHS RoB may be cause for disciplinary actions. Depending on the severity of the violation and management discretion, consequences may include one or more of the following actions:[3]

- Suspension of access privileges;
- Revocation of access to federal information, information systems, and/or facilities;
- Reprimand;
- Termination of employment;
- Removal or disbarment from work on federal contracts or projects;
- Monetary fines; and/or
- Criminal charges that may result in imprisonment.

HHS OpDivs may require users to acknowledge and comply with OpDiv-level policies and requirements, which may be more restrictive than the rules prescribed herein. Supplemental rules of behavior may be created for specific systems that require users to comply with rules beyond those contained in this document. In such cases users must also sign these supplemental rules of behavior prior to receiving access to these systems[4] and must comply with ongoing requirements of each individual system to retain access (such as re-acknowledging the system-specific rules by signature each year). System owners must document any additional system-specific rules of behavior and any recurring requirement to sign the respective acknowledgement in the security plan for their systems. Each OpDiv Chief Information Officer (CIO) must implement a process to obtain and retain the signed rules of behavior for such systems and must ensure that user access to such system information is prohibited without a signed.

[3] Refer to the Employee Standards of Conduct published by the U.S. Office of Government Ethics, available at: https://www2.oge.gov/web/oge.nsf/Employee%20Standards%20of%20Conduct

[4] National Institute of Standards and Technology (NIST) Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, defines an “information system” as: “A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.”

HHS Rules of Behavior 3

acknowledgement of system-specific rules and a signed acknowledgement of the HHS RoB.

National security systems, as defined by the Federal Information Security Management Act (FISMA), must independently or collectively implement their own system-specific rules.

These HHS RoB apply to local, network, and remote use[5] of HHS information (in both electronic and physical forms) and information systems by any individual.
Users of HHS information and systems must acknowledge the following statements:

I assert my understanding that:

- Use of HHS information and systems must comply with Department and OpDiv policies, standards, and applicable laws;
- Use for other than official assigned duties is subject to the *HHS Policy for Personal Use of IT Resources*, (as amended);[6]
- Unauthorized access to information or information systems is prohibited; and
- Users must prevent unauthorized disclosure or modification of sensitive information.[7]

[5] Refer to the glossary of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* for definitions of local, network, and remote access.
[6] *Available at: http://www.hhs.gov/ocio/policy/index.html*.
[7] HHS Memorandum: *Updated Departmental Standard for the Definition of Sensitive Information* (as amended) is available at: http://intranet.hhs.gov/it/cybersecurity/policies/index.html.

HHS Rules of Behavior 4

I must:

General Security Practices

- Follow HHS security practices whether working at my primary workplace or remotely;
- Accept that I will be held accountable for my actions while accessing and using HHS information and information systems;
- Ensure that I have appropriate authorization to install and use software, including downloaded software on HHS systems and that before doing so I will ensure that all such software is properly licensed, approved, and free of malicious code;
- Wear an identification badge (or badges, if applicable) at all times, except when they are being used for system access in federal facilities;
- Lock workstations and remove Personal Identity Verification (PIV) cards from systems when leaving them unattended;
- Use assigned unique identification and authentication mechanisms, including PIV cards, to access HHS systems and facilities;
- Complete security awareness training (i.e., HHS Information Systems Security Awareness Training) before accessing any HHS system and on an annual basis thereafter and complete any specialized role-based security or privacy training, as required by HHS policies;[8]
- Permit only authorized HHS users to use HHS equipment and/or software;
- Take all necessary precautions to protect HHS information assets[9] (including but not limited to hardware, software, personally identifiable information (PII), protected health information (PHI), and federal records [media neutral]) from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse, and treat such assets in accordance with any information handling policies;

[8] HHS Memorandum: *Role-Based Training (RBT) of Personnel with Significant Security Responsibilities* (available at: http://intranet.hhs.gov/it/cybersecurity/policies/index.html) defines the types of positions requiring specialized training.

[9] HHS IT assets are defined as hardware, software, systems, services, and related technology assets used to execute work on behalf of HHS. Definition is adapted from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments.

HHS Rules of Behavior 5

- Immediately report to the appropriate incident response organization or help desk (pursuant to OpDiv policy and/or procedures) all lost or stolen HHS equipment; known or suspected security incidents;[10] known or suspected information security policy violations or compromises; or suspicious activity in accordance with OpDiv procedures;
- Notify my OpDiv/StaffDiv Personnel Security Representative (PSR) when I plan to bring government-owned equipment on foreign travel (per requirements defined by the Office of Security and Strategic Information (OSSI));[11]
- Maintain awareness of risks involved with clicking on e-mail or text message web links; and
- Only use approved methods for accessing HHS information and HHS information systems.

Privacy

- Understand and consent to having no expectation of privacy while accessing HHS computers, networks, or e-mail;
- Collect information from members of the public only as required by my assigned duties and permitted by the Privacy Act of 1974, the Paperwork Reduction Act, and other relevant laws;
- Release information to members of the public including individuals or the media only as allowed by the scope of my duties and the law;
- Refrain from accessing information about individuals unless specifically authorized and required as part of my assigned duties;
- Use PII and PHI only for the purposes for which it was collected and consistent with conditions set forth by stated privacy notices such as those provided to individuals at the point of data collection and published System of Records Notices; and
- Ensure the accuracy, relevance, timeliness, and completeness of PII, as is reasonably necessary and to the extent possible, to assure fairness in making determinations about an individual.

[10] Known or suspected security incidents involve the actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information maintained by or in the possession of HHS or information processed by contractors and third-parties on behalf of HHS.

[11] OSSI policies for foreign travel can be found at: http://intranet.hhs.gov/training/foreign-travel-security-awareness/index.html

HHS Rules of Behavior 6

Sensitive Information

- Treat computer, network and web application account credentials as private sensitive information and refrain from sharing accounts;
- Secure sensitive information, regardless of media or format, when left unattended;
- Keep sensitive information out of sight when visitors are present;
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with the *HHS Policy for Records Management*[12] and sanitization policies, or as otherwise lawfully directed by management;
- Access sensitive information only when necessary to perform job functions; and
- Properly protect (e.g., encrypt) HHS sensitive information at all times while stored or in transmission, in accordance with the ***HHS Standard for Encryption of Computing Devices***.[13]

I must **not**:

- Violate, direct, or encourage others to violate HHS policies or procedures;
- Circumvent security safeguards, including violating security policies or procedures or reconfiguring systems, except as authorized;
- Use another person’s account, identity, password/passcode/PIN, or PIV card or share my password/passcode/PIN;
- Remove data or equipment from the agency premises without proper authorization;
- Use HHS information, systems, and hardware to send or post threatening, harassing, intimidating, or abusive material about others in public or private messages or forums;
- Exceed authorized access to sensitive information;
- Share or disclose sensitive information except as authorized and with formal agreements that ensure third-parties will adequately protect it;

[12] Available at: http://www.hhs.gov/ocio/policy/index.html

[13] Available at: http://intranet.hhs.gov/it/cybersecurity/policies/index.html

HHS Rules of Behavior 7

- Transport, transmit, e-mail, remotely access, or download sensitive information unless such action is explicitly permitted by the manager or owner of such information and appropriate safeguards are in place per HHS policies concerning sensitive information;
- Use sensitive information for anything other than the purpose for which it has been authorized;
- Access information for unauthorized purposes;
- Use sensitive HHS data for private gain or to misrepresent myself or HHS or for any other unauthorized purpose;
- Store sensitive information in public folders or other insecure physical or electronic storage locations;
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information;
- Copy or distribute intellectual property including music, software, documentation, and other copyrighted materials without written permission or license from the copyright owner;
- Modify or install software without prior proper approval per OpDiv procedures;
- Conduct official government business or transmit/store sensitive HHS information using non-authorized equipment or services; or
- Use systems (either government issued or non-government) without the following protections in place to access sensitive HHS information:
    - Antivirus software with the latest updates;
    - Anti-spyware and personal firewalls;
    - A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access; and
    - Approved encryption[14] to protect sensitive information stored on recordable media, including laptops, USB drives, and external disks; or transmitted or downloaded via e-mail or remote connections.

[14] Refer to the HHS Standard for Encryption of Computing Devices, available at: http://intranet.hhs.gov/it/cybersecurity/policies/index.html.

HHS Rules of Behavior 8

I must refrain from the following activities when using federal government systems, which are prohibited per the *HHS Policy for Personal Use of Information Technology Resources,*[15] (as amended):

- Unethical or illegal conduct;
- Sending or posting obscene or offensive material;
- Sending or forwarding chain letters, e-mail spam, inappropriate messages, or unapproved newsletters and broadcast messages;
- Sending messages supporting prohibited partisan political activity as restricted under the Hatch Act;[16]
- Conducting any commercial or for-profit activity;
- Using peer-to-peer (P2P) software except for secure tools approved in writing by the OpDiv CIO (or designee) to meet business or operational needs;
- Sending, retrieving, viewing, displaying, or printing sexually explicit, suggestive text or images, or other offensive material;
- Creating and/or operating unapproved Web sites or services;
- Allowing personal use of HHS resources to adversely affect HHS systems, services, and co-workers (such as using non-trivial amounts of storage space or bandwidth for personal digital photos, music, or video);
- Using the Internet or HHS workstation to play games or gamble; and
- Posting Department information to external newsgroups, social media and/other types of third-party website applications,[17] or other public forums without authority, including information which is at odds with departmental missions or positions. This includes any use that could create the perception that the communication was made in my official capacity as a federal government employee, unless I have previously obtained appropriate Department approval.

[15] Available at: http://www.hhs.gov/ocio/policy/index.html.

[16] For additional guidance refer to https://osc.gov/Pages/HatchAct.aspx and 5 C.F.R. Part 2635: Standards of ethical conduct for employees of the executive branch.

[17] Refer to the HHS Policy for Managing the Use of Third-Party Websites and Applications, available at http://www.hhs.gov/ocio/policy/index.html.

HHS Rules of Behavior 9

ACKNOWLEDGEMENT PAGE

By completing this course, I acknowledge that I have read the *HHS Rules of Behavior* (HHS RoB), version HHS-OCIO-2013-0003S,
dated July 24, 2013 (or as amended) and understand and agree to comply with its provisions. I understand that violations of the HHS RoB or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on Federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities; and may also include criminal penalties and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the OPDIV Chief Information Officer or his/her designee. I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

APPROVED BY AND EFFECTIVE ON:

________________/s/_______ ______________July 24, 2013___________

Frank Baitman DATE
HHS Chief Information Officer