LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

The Department of Health and Human Services Privacy Awareness Training

Fiscal Year 2015

Course Objectives

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

- Define privacy and explain its importance.
- Identify privacy laws, policies, guidance, and principles.
- Understand your role in protecting privacy and the consequences for violations.
- Define personally identifiable information (PII) and list examples.
- Protect PII in different contexts and formats.
- Recognize potential threats to privacy.
- Report a privacy incident.

Agenda

Module 1: Introduction to Privacy

Module 2: Protecting PII

Module 3: Threats to PII and Reporting

Module 4: Privacy References

Introduction to Privacy

MODULE ONE

Objectives

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

- Define privacy and understand the importance of privacy to the mission of HHS.
- Understand your role in protecting privacy and the consequences of a privacy violation.
- Identify privacy-related laws, guidance, and policies.
- Understand how privacy is put into practice.

What Is Privacy?

Privacy is a set of fair information practices to ensure:

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

Privacy also:

- Allows individuals a choice in how their information is used or disclosed.
- Assures that personal data will be used and viewed for business purposes only.
- Enables trust between HHS and the American public.

Roles and Responsibilities

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

Privacy policies and procedures require you to:

- 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 and computers.
- Report suspected privacy violations or incidents.

Possible Consequences of Privacy Violations

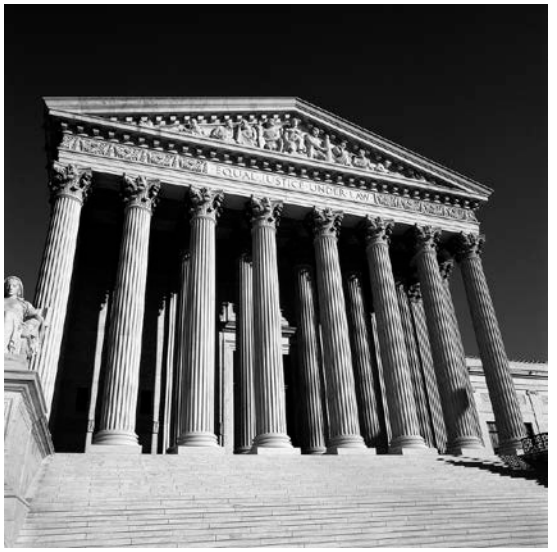
Privacy violations have several possible consequences:

- Employee discipline.
- Fines.
- Criminal charges.

Key Privacy Laws

Laws

- **Privacy Act of 1974**: Provides guidance for the collection, use, management, and disclosure of personal information.
- **E-Government Act 2002, Title II and III**: Requires federal agencies to assess impact of privacy for systems that collect information about members of the public.
- **Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule**: Restricts use and disclosure of protected health information (PHI) and grants individuals access to records.
- **Children's Online Privacy Protection Act (COPPA)**: Requires parental consent for certain Websites who knowingly collect personal information from children under the age of 13.



Key Privacy Guidance and Policy

Mandates

- **Office of Management and Budget M-07-16**: Requires safeguards for PII in electronic or paper format and policies and procedures for privacy incident reporting and handling.
- **National Institutes of Standards and Technology (NIST) Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations**: In Appendix J, NIST provides a structured, standardized set of privacy controls that all systems and organizations must address.

Policy

- **HHS-OCIO-2008-0001.003, Policy for Responding to Breaches of Personally Identifiable Information**: Establishes actions taken to identify, manage, and respond to suspected or confirmed incidents involving PII.

Visit http://www.hhs.gov/ocio/securityprivacy/index.html for a complete list of privacy guidance and policy.

Fair Information Practice Principles

HHS has long been a major force in establishing and meeting high standards for privacy. In 1973, HHS* advanced the Code of Fair Information Practice which has served as a foundation for future federal privacy frameworks.

Today, the framework most commonly employed asks that we think of privacy as having eight unique qualities.

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

* Formerly known as the Department of Health Education and Welfare (HEW)

** National Institutes of Standards and Technology Special Publication 800-53, Revision 4: Security and Privacy Controls for Systems and Organizations

Putting Privacy into Action

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

Framework	Description	Examples
Authority and Purpose	HHS provides the purpose for which the PII is collected at the time of collection, how the PII will be used, and the authority that permits the collection of PII.	▪Privacy Act Statements ▪System of Records Notices in Federal Register
Accountability, Audit, and Risk Management	Individuals have a clear understanding of their responsibilities for handling PII. Systems owners and program managers understand and 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 (cont.)

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 which guard against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.	▪Encryption ▪Shredding ▪User Names and passwords ▪Locks
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 which the information was collected except with the consent of the data subject; or by the authority of law.	▪PII collected for determination of benefits is not used for marketing

Protecting PII

MODULE TWO

Objectives

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

- Define PII and identify common examples of PII in the workplace.
- Identify privacy considerations throughout the information life cycle.
- Know how to protect PII in different contexts and formats.

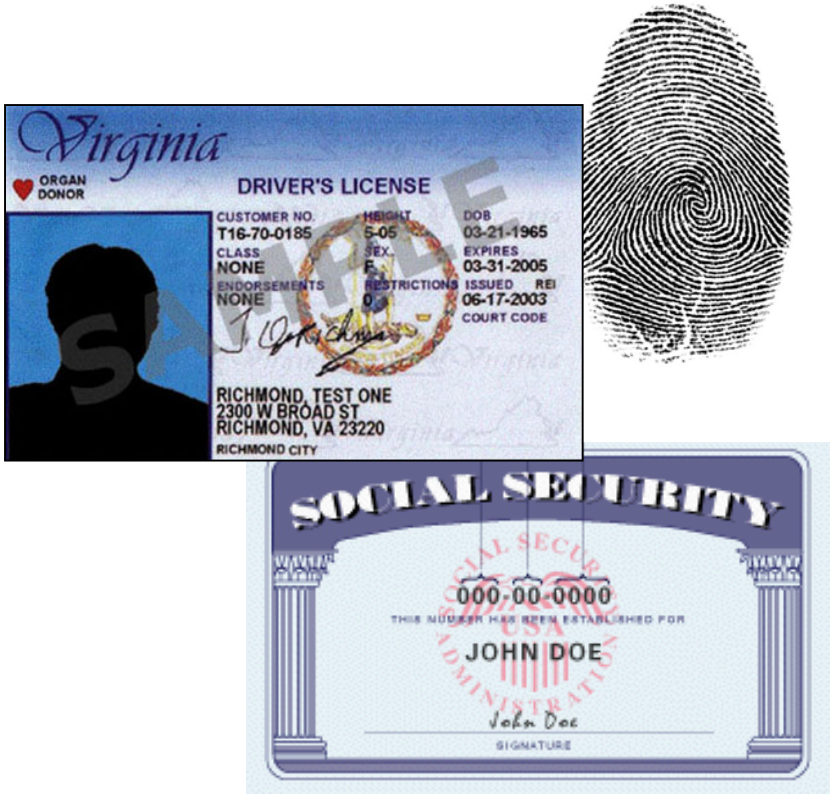
What is Personally Identifiable Information (PII)?

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

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

Common Examples of PII

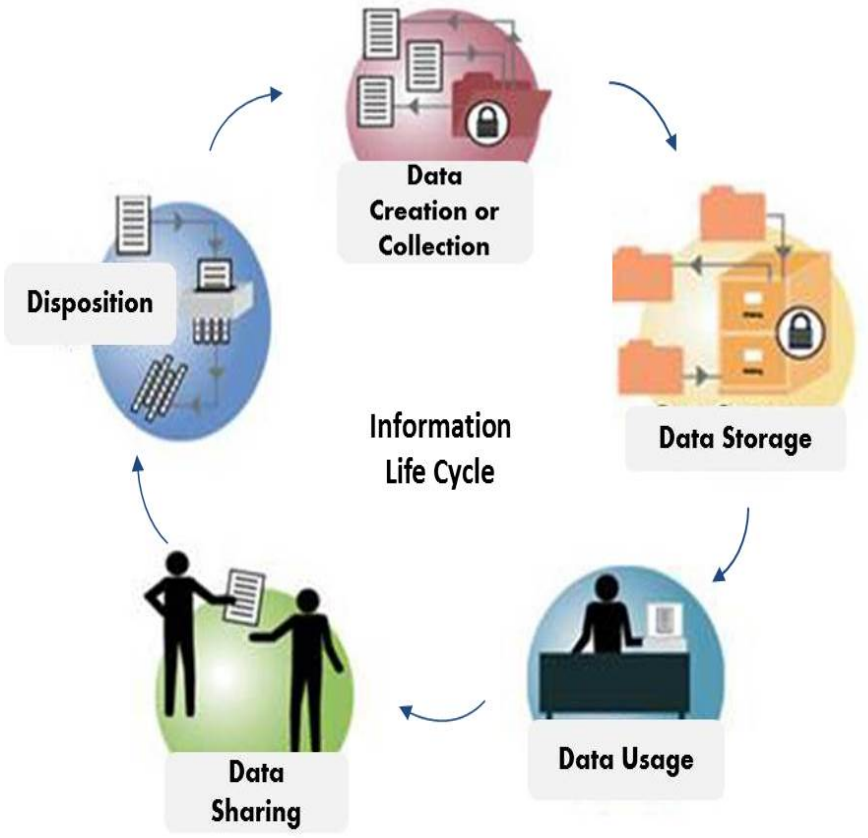
- Name
- Social Security number (SSN)
- Date of birth (DOB)
- Mother's maiden name
- Financial records
- Email address
- Driver's license number
- Passport number
- Health information



PII Considerations for the Information Life Cycle

The Information Life Cycle defines how to handle data from inception to disposition. Protecting PII is important during each stage of the information life cycle:

- **Data Collection or Creation**: Gathering PII for use.
- **Data Storage**: Maintaining or storing PII.
- **Data Usage**: Using PII to accomplish a job function.
- **Data Sharing**: Disclosing or transferring PII.
- **Disposition**: Disposing of PII when no longer needed in accordance with record management requirements and organizational disposal policies.



PII Considerations for the Information Life Cycle (cont.)

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

Did you shred all papers containing PII?

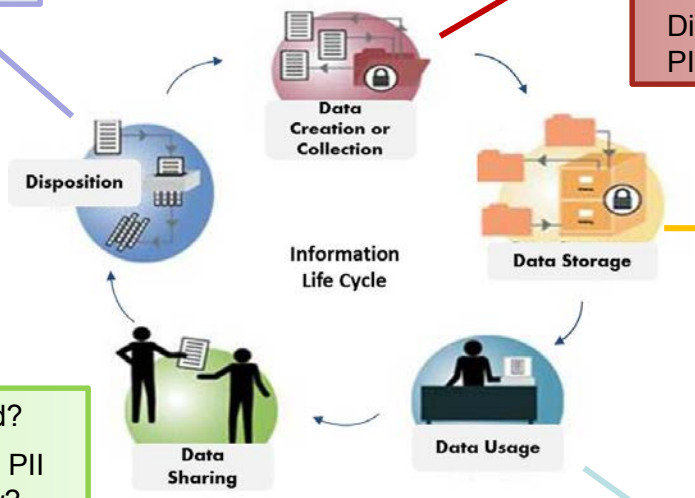
Did you give back unused equipment (e.g. computer, copiers, fax machines) to the IT Department for proper disposal?

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 secure documents and files that contain PII?

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

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

Did you verify that the sharing is allowed?

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

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

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

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

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

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

Protect PII: Lock-It-Up

Personnel are required to protect PII in their possession.[1] The following will help you keep PII safe from unintended use or disclosure.

Physical Protection

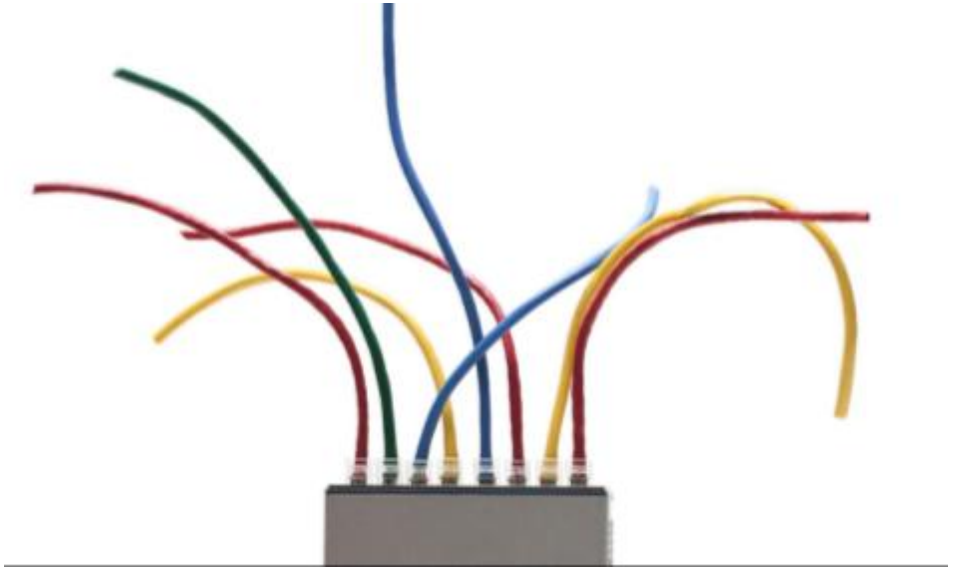
- Lock your computer workstation (CTRL + ALT + DELETE).
- Lock up portable devices (e.g., laptops, cell phones).
- Remove the Personal Identity Verification (PIV) card when you are away from your computer.
- Lock up documents and files that contain PII.

[1] See HHS Policy for Personal Use of Information Technology Resources

Protect PII: Protections in Transit

Protect PII during transit.

- Encrypt emails that contain PII.
- Use an authorized mobile device with encryption to store PII.
- Don’t forward work emails with PII to personal accounts (e.g., Yahoo, Gmail).
- Don’t upload PII to unauthorized Websites (e.g., Wikis).



Protect PII: Protections During Travel

When travelling, keep equipment and papers that contain PII in your possession.

- Do not place it in checked baggage or leave it in the trunk of a car.
- Avoid leaving it in a hotel room unsupervised (e.g., use hotel safe).
- Remember to pick up your laptop after the TSA security check at the airport.

Protect PII: Clean-It-Up

Maintain a clean work environment.

- Don’t leave documents that contain PII on printers and fax machines.
- Don’t leave files or documents containing PII unsecured on your desk when you are not there.

Protect PII: Faxing

Before faxing:

- 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.

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.

Protect PII: Mail

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.

Protect PII: Encryption

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 in the same email as the encrypted file.
- Give the password either in person, over the phone, or if necessary, send in a separate email.

Protect PII: Telework

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.[1]
- Store sensitive information on authorized mobile devices or remote systems with appropriate safeguards (e.g., HHS encryption).[2]
- Remotely access sensitive information by using authorized methods (e.g., Virtual Private Network (VPN)).

Work with your manager for approval and to ensure that your equipment has safeguards in place to protect sensitive information during telework.

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

Protect PII: SSN Protections

Employees that 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.
- Documents containing SSNs should be locked up and put away so they are not left out when away from your desk.
- Identify and implement ways to eliminate the use of SSNs, when possible (e.g., removal from forms, assigning a randomly generated identifier).

Protect PII: Disposition

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

Protect PII: Beware of Phishing

Phishing is an attempt to steal personal information. Most times it involves an e-mail, although other forms of communication can be used, which claims to be a legitimate business or person in an attempt to scam you into surrendering PII or downloading malicious software.

Be suspicious of any email that:

- You were not expecting to receive.
- Requests your PII (account numbers, SSN, username, passwords, birth date, etc.).
- Requires you to urgently take action (e.g., verify your account or log-in to prevent your account from being closed).
- Does not look like a legitimate business Website (e.g. logos look funny, spelling errors).
- Has a different URL than the one you are familiar.
- Contains a document that shuts down and re-launches after you open it.

Protect PII: Beware of Phishing (cont.)

On the right, are some examples of phishing e-mails. Take the following actions if you believe you received an e-mail that is a phishing attempt:

- Do not respond to phishing emails.
- Delete suspected phishing emails.
- Do not open attachments in phishing emails.
- Do not click hyperlinks in a phishing email.
- Contact the Help Desk if you think you have responded to a phishing email.

From: Internal Revenue Service [mailto:admin@irs.gov]
Sent: Wednesday, June 15, 2013 12:45 PM
To: john.doe@jdoe.com
Subject: IRS Notification - Please Read This

From: Your Bank [mailto:iseamab@hotmail.com]
Sent: Friday, July 29, 2013 2:45 PM
To: john.doe@jdoe.com
Subject: Urgent - Your Account is Going to Expire.

From: Your Manager [mailto:axilwohan147@yahoo.com]
Sent: Tuesday, July 26, 2013 2:13 AM
To: john.doe@jdoe.com
Subject: Check out these funney pickters!

Threats to PII and Reporting

MODULE THREE

Objectives

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

- Recognize an incident of privacy and identify common scenarios.
- Understand the effect of a privacy compromise.
- Report suspected incidents.

What is a Privacy Incident?

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

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

Common Scenarios

Privacy incidents most often occur from:

- Loss, damage, theft, or improper disposal of equipment, media, or papers containing PII.
- Accidentally sending a report containing PII to a person not authorized to view the report or sending it in an unprotected manner (e.g., unencrypted).
- Allowing an unauthorized person to use your computer or credentials to access PII.
- Discussing work related information, such as a person's medical health records, in a public area.
- Accessing the private records of friends, neighbors, celebrities, or any other person when not authorized to do so.
- Any security situation that could compromise PII (e.g., virus, phishing email, social engineering attack).

Effects of Compromised Privacy

Loss of privacy threatens people and HHS. It can result in:

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

"Washington State system hacked, data of thousands at risk"

Reuters, May 9, 2013

"Chinese Hackers Infiltrate New York Times Computers"

New York Times, January 30, 2013

"Personal information stolen from Michigan Department of Community Health website"

The Detroit News, July 5, 2013

How to Report

- Do not investigate the incident on your own - immediately report suspected incidents that could compromise PII in any format (electronic, paper, or oral communications).
- 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.
- Report incidents to your OpDiv Computer Security Incident Response Team (CSIRT)/Incident Response Team (IRT). Contact information for each OpDiv can be found at: http://intranet.hhs.gov/it/cybersecurity/hhs_csirc/
- You can also report directly to the HHS CSIRC by email csirc@hhs.gov or phone 866-646-7514.
- 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).

Privacy References

MODULE FOUR

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).

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.

Report a privacy incident to the OPDIV CSIRT (http://intranet.hhs.gov/it/cybersecurity/hhs_csirc/index.html) or HHS CSIRC CSIRC@hhs.gov or 1-866-646-7514.

Course Summary

You should now be able to:

- Define privacy and explain its importance.
- Identify privacy laws, policies, guidance, and principles.
- Understand your role in protecting privacy and the consequences for violations.
- Define PII and list examples.
- Protect PII in different contexts and formats.
- Recognize potential threats to privacy.
- Report a privacy incident.