US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

01/05/2015

OPDIV:

NIH

Name:

Information Security Privacy Awareness Training

PIA Unique Identifier:

P-6597382-541693

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

N/A

Describe the purpose of the system.

The NIH security and privacy awareness website contains a variety of courses which pertain to annual information security awareness, privacy awareness, securing remote computers, completing refresher requirements, etc. The security awareness training is required for NIH staff and other persons who use NIH IT resources. The system allows individuals to self-record role-based training and accept (agree to adhere to) the NIH IT General Rules of Behavior, Remote Access and Mobile Device User Agreements.

Describe the type of information the system will collect, maintain (store), or share.

Training verification information (name, HHS badge number, organization, work email address, employment type, student record and dates the modules were completed by the user).

Provide an overview of the system and describe the information it will collect, maintain (store), or share.

The training course requires that NIH users log onto the course using their HHS Badge Number. The progress of members of the public is not tracked but they can enter their name to appear on the certification of completion.

The tracking system exists to allow NIH to retain a record of user training and agreements to follow the NIH IT General Rules of Behavior, Remote Access and Mobile Device policies. Individual student record information is not disseminated. Compliance statistics are reported to HHS and OMB in the aggregate.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

HHS Badge Number

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Public Citizens

Vendor/Suppliers/Contractors

Staff listed in the NIH Employee Directory (NED) with access to IT equipment and resources.

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

Information about the status of training completion may be shared with supervisors for the purpose of reporting non-compliance with the mandatory requirement to complete the training within the specified timeframe.

Describe the secondary uses for which the PII will be used.

No secondary use

Identify legal authorities governing information use and disclosure specific to the system and program.

42 USC 241 and 282 and E.O. 9397

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

NIH 09-25-0216, NIH Electronic Directory

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

N/A

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

When they access the website, staff are asked to provide their name and HHS badge number to track training completion.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

There is no option to object to logging into the system with a name and badge number. They are necessary for the system to track course completion and NIH to report training metrics to HHS.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

There is no process to notify and obtain consent. NIH must log into the training system with their name and badge number in order to receive credit for course completion and for NIH to ensure compliance. The name and badge number are validated by the NIH Employee Directory which is a separate system that obtains consent when changes occur.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

The user is informed to contact the IT Service Desk or their Institute/Center (IC) Information Systems Security Officer (ISSO) or Privacy Coordinator with questions or concerns.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

None. Name and HHS badge number are pulled from the NIH Employee Directory for the purpose of monitoring training completion. NED is the authoritative source for PII.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Users can see their own data

Administrators:

To track training

Developers:

To enhance course

Contractors:

To modify course

Others:

Supervisors - To review training completion

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

There are different levels of access depending on the role of the individual accessing the tracking system. These roles include System Administrator and Institute/Center-specific access for Information Systems Security Officers and Privacy Coordinators, with or without authorization capability, read-only and authorize capability.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

The need for ongoing access to this on-line tracking system is verified annually. When a person leaves or they are no longer considered to need access, they are made inactive and can no longer access the data.

The type of role assigned to users is based on a business need and request by the relevant Institute/Center Information Systems Security Officer and Privacy Coordinator.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

All NIH staff, to include those with access to the system for the purpose of tracking are required to complete the Entire Information Security and Privacy Awareness Training courses as well as the Combined Annual Refresher.

Describe training system users receive (above and beyond general security and privacy awareness training).

N/A

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

NIH Manual Chapter 1743 - Keeping and Destroying Records, Section 2300-410 deals with training records. The general files of NIH-sponsored training are to be destroyed 5 years after completion of a specific training program.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

From a User's perspective: Any user can log into the training website and view their Student Record, which provides completion information (i.e., dates modules/courses were completed). If they have any concerns about the recordation process, they can contact the NIH IT Service Desk.

From the Administrator perspective: There are different levels of access depending on the role of the individual accessing the tracking system. These roles include administrator privileges, Institute/Center-specific access with or without authorization capability, read-only and authorize capability. A unique 10-character password is required to access the tracking system.

The system is hosted on the NIH server behind the firewall. There is a time-out feature for inactivity (15 minutes) requiring the user to log back into the system.

Identify the publicly-available URL:

http://irtsectraining.nih.gov

Does the website have a posted privacy notice?

No

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null