US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/16/2025

OPDIV:

CMS

Name:

Information Technology Security and Privacy - Computer Based Training

PIA Unique Identifier:

P-4374608-973680

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

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

No

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

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

PIA Validation

Other: Software as a Service (SaaS) system integration

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

A new Federal Risk and Management Program (FedRAMP) approved (Software as a Service) SaaS application has been introduced which will in the next few months transition ITSP-CBT from on prem to cloud.

Describe the purpose of the system.

Information Technology Security and Privacy - Computer Based Training (ITSP-CBT) System stores training information for the annual CMS Information Security and Privacy program.

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

ITSP-CBT collects and maintains name, phone numbers, e-mail address, user IDs and training completion dates. The system doesn't collect any other user credentials and utilizes the userid to uniquely identify the record within the system.

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

The system provides both CMS employees, direct contractors, federal and state agencies with the required Information Security and Privacy Training via a computer-based training module. The ITSP-CBT System regularly uses PII to retrieve system records for internal reporting purposes including using the first name, last name, EUA ID, and/or email address of CMS employees and contractors. User ID is required to uniquely identify the user in Information Technology Security and Privacy - Computer Based Training (ITSP-CBT) System. Other general information such as Name, Email Address, Phone Number, training completion dates are used for internal reporting on the training status.

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

Yes

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

Name
E-Mail Address
Phone Numbers
Education Records
Other: User ID

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

Employees
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

Information is shared with the Enterprise User Administration system (EUA) database for the purpose of verifying users that are taking or have taken the required security awareness CBT. CBT is required for initial access to CMS systems and as part of annual system certification.

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

Personally Identifiable Information (PII) such as name, official email address is utilized in reports to keep track of the Information System Security and Privacy Awareness (ISSPA) training completed by the CMS user.

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

42 CFR 401.101–401.148 and sec 1106(a) of the Social Security Act, 42 U.S.C. 1306(a)

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.

09-90-1901 - HHS Correspondence, Comment, Customer Service, and Contact List Records

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

Not Applicable

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.

No prior notice is given as the system doesn't directly collect any personal information. The information is provided by the EUA on a nightly basis as a data extract and CBT system only stores the minimum information needed to identify a CMS user and generate reports on training.

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.

The PII that is collected is in a separate application, which is the EUA, therefore there is no ability to opt-out.

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

Notification is not provided by ITSP-CBT, because the PII is not directly collected from the individual.

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 PII data is obtained from another CMS System, therefore, there is no process in place by CBT to address individual's 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.

The PII data is obtained from another CMS System, therefore, the process to ensure PII is not improperly or inadvertently modified or destroyed is by only allowing system administrators to have access to the database containing PII. The PII fields are locked and cannot be changed; The process to ensure that individuals who provide or modify PII cannot repudiate that action is done within the source (EUA) system. The process to ensure PII is available when needed is by having nightly updates run between the EUA systems and ITSP-CBT; the process to ensure that PII is sufficiently accurate for the purposes needed is ensured when the nightly updates are sync.

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

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

Access to Personally Identifiable Information (PII) within the system is granted based on the principles of least privilege and need-to-know, in accordance with CMS Information Security and Privacy policies. System users (e.g., administrators, developers, contractors) must receive prior approval from the Information System Security Officer (ISSO) before being granted access to PII. Access requests are documented and reviewed in alignment with the procedures defined in the Information Technology Security & Privacy – Computer-Based Training (ITSP-CBT) Operations & Maintenance Manual (OMM).The ISSO performs regular (at least quarterly) account reviews to identify and remove unnecessary or inactive accounts and to validate that access remains appropriate for each user's role. Any changes in user roles or responsibilities trigger a re-evaluation of their access privileges. Additionally, all users must complete mandatory Information System Security and Privacy Awareness (ISSPA) training prior to receiving access, to ensure they are aware of their responsibilities for protecting sensitive information.

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.

Role based access is provided to those having access to PII and is limited to a 'need to know' basis and access is granted per their user identification.

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.

Annual Information System Security & Privacy Awareness (ISSPA) training is mandatory for all personnel who have access to Personally Identifiable Information (PII), including but not limited to the System Owner, System Developer Maintainer, CBT Admin Team, and Database Administrator. The training covers topics required to protect sensitive data and ensure compliance with CMS Information System Security and Privacy policies. These responsibilities align with NARA's General Records Schedules (GRS), including: GRS 3.1 – Information Access and Protection Records, which governs records related to information access controls, user permissions, and awareness of access responsibilities; and GRS 3.2 – Information Systems Security Records, which includes records related to cybersecurity training, system security planning, incident response, and ongoing security awareness activities. All personnel must complete this training annually as part of CMS's continuous compliance efforts with FISMA and HHS security and privacy requirements.

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

Other training avenues such as conferences, seminars and classroom training provided by CMS/HHS are available apart from the regular annual training.

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.

CMS follows the requirements listed in the National Archives and Records Administration (NARA) policy, specifically Chapter 8 – Information Technology, Sub-chapter: Information Technology Security. While earlier practices referenced GRS 20 and GRS 24, these have since been retired. CMS now complies with the updated General Records Schedules, including:GRS 3.1 – General Technology Management Records GRS 3.2 – Information Systems Security Records GRS 5.2 – Transitory and Intermediary Records. These schedules provide the current federal guidelines for the retention and destruction of electronic records containing Personally Identifiable Information (PII), which CMS follows in conjunction with internal policies to ensure secure data life-cycle management.

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

The administrative, technical, and physical controls documented in the CMS Information Security ARS - Appendix B CMSR Moderate Impact Level Data shall be applied to this system. PII information is pulled from EUA daily. EUA manages the validity of PII and no changes on PII are made on the CBT end. The administrative controls for system backup, contingency planning and training are applied. Real backup data is used in the restoration of information system functions as part of contingency plan testing. Backup information is securely stored offsite in a facility managed by Iron Mountain. The technical controls for authorized access to the system, least privileges, and password and incident management are applied. The physical controls in place consist of security guards, identification badges, key cards, cipher locks and closed-circuit TV are applied.

Note: web address is a hyperlink.