

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/29/2016

OPDIV:

CMS

Name:

CMS Administrative Technology Solutions

PIA Unique Identifier:

P-1455650-887315

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

Conversion

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

The CMS Administrative Technology Solutions (CATS) system was implemented on October 15, 2012 and is currently in the Operations and Maintenance phase of the life cycle. No changes in the system.

Describe the purpose of the system.

The CMS Office of Support Services and Operations (OSSO) CMS Administrative Technology Solutions (CATS) system automates personnel related processes which involve all CMS employees. For example, it allows employees to request the ability to work remotely or submit suggestions or apply for 'work details'. It also provides a place for managers to delegate tasks, input performance appraisals and claim/release employees that they manage.

CATS is an internal CMS system that is only accessible by CMS employees and when an employee

is logged onto the CMS intranet. By automating human resource and administrative processes, CATS provides some operational cost-savings to CMS.

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

The CATS system contains the following information about CMS employees: employee name, SSN (obfuscated, never displayed to users), address, date of birth, employment status and information (position, tier, manager information, employee ID number), Automobile license plate information and educational information. It also contains user ID and passwords of employees, job-related task information and the user credentials for the system support staff to access the system.

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

The CATS system is an internal CMS IT system that is only accessible by employees to perform job-related functions and to access some CMS internal resources. While all CMS employees can access CATS, the level of available resources or functions are determined by the employee's position, i.e., whether a manager, an officer, administrator, or other position.

The system has automated the following human resource and administrative-related task areas: employees may apply for a work detail; report and file ethics forms and make employee designations; employees may submit suggestions; area to apply for CMS sponsored activities such as the flu-shot program and blood drives; there is an Executive Officer listing for all CMS components; employees may request a remote work schedule; managers can perform annual self-assessments; employees can request mentors or mentees; managers can claim and/or release CMS employees within CATS; Executive Officers can assign temporary managers; employees within Office of Hearings can track hearing cases; Human Resource employees can generate position description numbers; and managers can create and generate performance plans for CMS employees.

Additionally, there is a report-generation function for managers and other designated employees to run reports about all of these task areas.

The information about CMS employees is collected by and transferred from the HHS personnel system, Capital Human Resources (CapHR) to CMS' Division of Administrative and Systems Management (DASM) and it is uploaded into CATS on a bi-weekly basis to update the information. Information is retained within CATS for the length of employment.

When CMS employees access the system, they input their user ID and password. These are not created within CATS but within the Enterprise User Administration (EUA) system. The EUA system assigns the permission to access CATS.

It has its own PIA for the PII that is collected and maintained within it.

The CATS system support staff accesses the system with their user ID and password, which was also created within EUA.

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

Yes

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

Social Security Number

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Education Records

Employment Status

Other - User ID, Password, Automobile license plate information, employment information, employee

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

Employees

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

The data is used to identify employees' credentials to access CATS.

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

Not applicable

Describe the function of the SSN.

Formerly, the SSN was used to identify an employee. However, that is no longer the case, it is now just stored as part of an employee's personnel data.

Cite the legal authority to use the SSN.

Executive Order 9397, the Debt Collection Improvement Act, 31 United States Code (U.S.C.) §7701 (c)(1), and 5 U.S.C. 552a(b)(1)

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

Executive Order 9397, the Debt Collection Improvement Act, 31 United States Code (U.S.C.) §7701 (c)(1), and 5 U.S.C. 552a(b)(1)

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.

09-70-0538, Individuals Authorized Access to CMS Computer Services (IACS), published 7/26/2002

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

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.

CMS employees' information is uploaded into CATS from the CapHR system; therefore there is no notice from CATS that their personal information is being collected. However, to log into the CATS system, an employee is presented with a 'warning banner' that advises of the collection of PII and includes an acknowledgement of the CATS Rules of Behavior that the individual must agree to prior to accessing the system.

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 isn't a way for an individual to 'opt out' of providing their PII because it is required to access the CATS system. Additionally, the individual CMS employee's information is uploaded into CATS as part of the employment process, from the HHS CapHR system.

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

If there is a change in the way PII is collected and used by CMS, employees would be notified by the CapHR system and other notification methods, outside of the CATS system. If there are changes to the way that employees log into CATS with their user ID and password, the 'warning banner' and Rules of Behavior would be updated and provided to CMS employees.

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.

If the PII is inaccurate, the CATS user can contact the CATS Help-desk or DASM. If a CATS user believes their PII has been obtained, used or disclosed inappropriately they can report it to the CMS IT help desk, who would investigate and provide steps for resolution of the concern.

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

When the PII data comes from CapHR, it is compared within CATS by the EUA system for accuracy, relevancy, availability and integrity. If there are any anomalies, then the CATS profile will not be created. An error message alert would be sent to the individual. Corrections to PII are done through coordination between the user, EUA, and CapHR. CATS error logs are reviewed daily and any questionable PII information is addressed with the user, the DASM, CapHR and the Governmental Task Lead (GTL) for CATS.

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

Users:

Only authorized users, managers, directors and other higher level staff, may have access to PII. Access is for creating reports, assigning tasks and other management-related tasks.

Administrators:

System administrators do not have access to PII. However, some users with an Administrator role may access PII for reporting and other functions relating to the management of information and tasks.

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

CATS system access is role-based so that only the least amount of PII is displayed based on the employees role. For instance, employees cannot see what managers see. Access to reports must be approved by the business owner who determines what report data may be shared.

Administrators/Business owners can only see their task data.

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.

CATS system access is role-based and based on "least privilege" so the users only have access to a limited amount of PII, based on their role and/ or tasks. For instance, employees cannot see what managers see. Access to reports must be approved by the business owner who determines what report data may be shared. Administrators/Business owners can only see their task data. All test environments are obfuscated to remove PII. Developers can only update code.

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 CMS employees are required to complete the mandatory annual Security and Privacy Awareness Computer Based Training (CBT). Completion of the training is confirmed by a test taken at the end of the training and the results/certificate is recorded in the CBT database.

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

Additionally, all CMS employees with significant information security responsibilities are required to complete role-based training. The OOM's Information System Security Officer (ISSO) works closely with other CMS department managers and employees to ensure that OOM is regularly informed of any necessary security requirements and that department remains compliant with all CMS guidelines and regulations.

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.

CATS follows the CMS Record Schedule published April 2015 which references the National Archives and Records Administration's (NARA) General Record Schedules (GRS) 1, which states that records will be destroyed from a minimum of 6 months (interview records) or retained as long as 7 years (grievance-related).

CMS will retain information, subject to the GRS or for the duration the user needs access to CMS' computer systems or until no longer needed for administrative, legal, audit or other operations services, whichever is longer. All claims-related records are encompassed by the document preservation order and will be retained until notification is received to take further action.

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

The administrative controls in place are that information can only be accessed by authorized personnel. Authorized persons can only access the system by using their CMS issued ID and a password. There are role-based accessibility controls that limit the amount of information available on an 'as required' and least privilege rule.

All passwords are changed every 60 days or the person will be locked out of the workstation.

Their workstation can only be unlocked by calling the Action Desk after verifying a person's identity. The CATS system as well as the employee's workstation will shut down after a certain period of inactivity and only the person that was logged into the system will be able to unlock the computer. The information is encrypted in transfer from CapHR to CATS and The system is stored in a Data Center and accessed via the CMS intranet only, which is protected by firewalls which secures the information from intruders.

The physical controls that are in place such as the security guards ensure that access to the building (s) are only granted to authorized individuals. The identification of everyone that enters the facility is checked and there is video monitoring.