

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/02/2016

OPDIV:

CMS

Name:

CMS Issue Tracking System

PIA Unique Identifier:

P-1095015-766226

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.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.**Describe the purpose of the system.**

The CMS Issue Tracking System, also known as "Remedy", is a ticketing system used to track information technology (IT) service requests, incidents, problems, infrastructure change requests, work orders, tasks, assets, and other business service management data. Remedy is a web based application used within Web browsers. Remedy is the primary application for tracking IT related requests for the Centers for Medicare & Medicaid Services (CMS).

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

The Remedy application collects, maintains and stores sensitive information technology data such as Internetwork Protocol (IP) addresses, operating system versions and patch levels, security incidents such as data breaches, and personally identifiable information about CMS information system users; direct contractors and CMS government employees, including their employment status as a contractor or government employee. User names and passwords are passed through the Remedy application to the Enterprise User Administration (EUA) system in order for users to authenticate and make use of Remedy. EUA has its own separate PIA. Users may be associated to user name by their actual full names in order to open, track, and resolve incident tickets.

While PII is not required for an issue to be logged, Point of Contact information (email address and phone numbers) will be requested for tracking progress of the issue being remediated. Users are able to enter or communicate to help desk personnel (direct contractors) any information pertinent to the incident, including PII or other data that may be sensitive.

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

The Remedy application collects, maintains and stores sensitive information technology data such as Internet Protocol (IP) addresses, operating system versions and patch levels, security incidents such as data breaches, and personally identifiable information (employment status) about CMS information system users. The data is used to create, track and monitor IT service requests, incidents, problems, infrastructure change requests, work orders, tasks, and assets. The reporting environment enables authorized users; direct contractors and CMS government employees, to generate reports based on criteria fields about the tickets stored within the application. This information is used for internal purposes only and is not shared with third parties.

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

Employment Status

Other - User names, passwords, IP Addresses

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

Other - Any person who calls into the CMS Help Desk to report an issue or concern has the option of providing PII, or any other information pertinent to an issue or incident, to a CMS Help Desk representative. It is not typical for individuals outside of CMS or its vendors, suppliers, or contractors to report issues, however, it is possible.

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

PII is used to uniquely identify CMS information system users and correlate them to Remedy ticket information.

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

None

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

Title 5 U.S. Code, Section 552a(e)(10)

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.

A SORN is being developed.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

Remedy does not require the collection of information which is subject to the Paperwork Reduction Act. Users, under their own discretion, may provide information for troubleshooting information technology issues.

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.

Personal information is only collected at the time that the CMS employee, direct contractor, or affiliate applies for access to the system. Page 3 of Application for Access to CMS Systems informs individuals that their PII is being collected and the purposes for collecting the PII. Users are authenticated via the Enterprise User Administration system, and as such, Remedy does not collect PII directly from users for authentication purposes.

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.

In order for users to gain access to the Remedy application, users must fill out the appropriate paperwork to receive an Enterprise User Administration (EUA) account with the correct job codes. The request for an EUA account states, "Furnishing the information on this form, including your Social Security Number, is voluntary. However, if you do not provide this information, you will not be granted access to CMS computer systems."

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

All users must recertify their access within every 365 days. By doing so the user are consenting to the continued use of their PII. PII will only be used for the purposes given at the time of collection. PII will only be used as necessary in performance of job duties.

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.

Users can call the CMS Help Desk to report issues regarding their PII being inappropriately obtained, used, or disclosed, or to update their PII. The existing CMS privacy breach process as documented in the CMS Risk Management Handbook Volume is followed for any potential information security incident.

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

Remedy is not used as a system of record or used to update any PII attributed to users. PII is used by Help Desk personnel to identify points of contact for return calls related to information system or information technology related issues. Point of contact information is verified during the issue remediation process by Help Desk personnel. Help Desk personnel ask for the user's contact information during each engagement, even if the information has already been provided in previous calls or engagements.

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

Users:

Remedy users will have access to PII as a part of the verification process when processing incident tickets for resolution. PII is used to verify the identity of the individual submitting incident details. Users will have read access to their own PII, as well as the PII of other government employees and contractors.

Administrators:

Database and Remedy Application administrators may have access to PII due to the level of privilege associated with their database accounts. These privileges are needed in order to maintain the database and application so it can function properly and securely. Administrators will have read and write access to any PII stored in Remedy.

Contractors:

These contractors are direct contractors that function in capacities which require access to PII within Remedy. Direct contractors can be administrators or non-privileged user of the Remedy application, and require access to PII for the aforementioned reasons. Additionally, direct contractors may act in a security role to respond to and relay information about information security incidents whereby they must share this information with other direct contractors within HHS. The sharing of this information is for official investigation use only.

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

The Remedy application has built in role and permission schemes which have been tailored to fit the needs of CMS. During that process, the use of PII was determined to be appropriate for internal business uses only, for verification of identity and for possible security incident investigations. It was determined that only Administrators and two specific user communities require access to PII. Help Desk Users need access to PII for verification purposes to reset other Users' passwords. Database Administrators have access to PII in order to maintain the database which stores the PII. Contractors are a part of the Administrator, Help Desk, and Database user communities.

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.

All activity within the Remedy application is subject to audit logging and monitoring. Any modification of ticket data, including any PII information, is traceable back to an individual that last made a change to the ticket, via a user name and timestamp associated with the activity. Direct access to databases which may contain PII are subject to a logging and monitoring process which details any user selection or modification of data by means other than the use of Remedy application. Additionally, only database administrators are given direct logical access to the Remedy database. All other system and application user accounts do not have approval, authorization, or the logical permissions necessary to alter or manipulate the information within the database directly.

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.

CMS Security Awareness and Privacy training is provided to each user on an annual basis. Users acknowledge successful training after passing test at the end of training and the system verifies completion. Included in the training is education about how to properly handle sensitive data.

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

Not applicable.

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.

The following processes and guidelines are adhered to in the retention and destruction of data: CMS Record Schedules - N1-440-10-6, Item 1, N1-440-10-6, Item 2, N1-440-10-6, Item 3.

The general disposition authority for correspondence within remedy can be aligned to the CMS Record Schedule dated April 2015, III. MEDICARE RECORDS--PROGRAM RELATED, Item Q. Routine Inquiries/Correspondence. This type of information accumulates as a result of a wide-range of correspondence, inquiries and complaints from beneficiaries, providers, etc., that are received by CMS headquarters, regional offices, and Medicare contractors.

DISPOSITION:

3. Inquiries/Correspondence - (Official Recordkeeping Copy). Response requires additional research staff or time.

Destroy 5 years after the date of the response to the correspondence, or when no longer needed for Agency business, whichever is longer. (Disposition Authority: N1-440-10-6, Item 1)

4. Inquiries /Correspondence – (Official Recordkeeping Copy).

Response requires little effort on the part of CMS staff for response. Destroy 2 years after the date of the response to the correspondence, or when no longer needed for Agency business, whichever is longer. (Disposition Authority: N1-440-10-6, Item 2)

5. Inquiries /Correspondence - No Response Required

Destroy 3 months after the date of the incoming correspondence, or when no longer needed for Agency business, whichever is longer. (Disposition Authority: N1-440-10-6, Item 3)

For potentially sensitive and/or security related information:

CMS retains records to facilitate the review of PII disclosures/access records for five (5) years. CMS ensures that audit information is archived for six (6) years to enable the recreation of computer related accesses to both the operation system and the application wherever PII is stored. CMS retains PII inspection reports, including a record of corrective actions, for a minimum of three (3) years from the date the inspection was completed. CMS retains electronic records for 1 year to provide support for after-the-fact investigations of security incidents and to meet regulatory and CMS information retention requirements. CMS record retention requirements are updated to meet the requirements of The National Archives and Records Administration (NARA) General Records Schedules. When PII is destroyed, CMS follows the guidance of NIST Special Publication 800-88 Rev. 1. CMS will disintegrate, pulverize, melt, incinerate, and/or shred PII data once it is no longer necessary to retain. Certificates of destruction are completed and retained whenever PII data is destroyed.

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

To ensure the security and privacy of sensitive information in Federal computer systems, the Computer Security Act of 1987 requires agencies to identify sensitive computer systems, conduct computer security training, and develop computer security plans. CMS maintains a system of records for use in assigning, controlling, tracking, and reporting authorized access to and use of CMS computerized information and resources.

The Remedy application is subject to the CMS Security Assessment and Authorization (SA&A) process. Security documentation describing how the Acceptable Risk Safeguard (ARS) controls are implemented is stored within the CMS FISMA Control System (CFACTS). CMS includes the privacy artifacts required in the CMS expedited Life Cycle (XLC) and highlighted in the Privacy-Enhanced System Design and Development section of the Risk Management Handbook for Privacy.

The Remedy application development methodology includes privacy requirements considerations throughout the design and implementation process. Risk score cards are completed and maintained for the system development and changes which may impact the security of the information within the application. Prior to logging into the Remedy application, a system use notification message banner is displayed. This notification provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Once a user is logged into Remedy, the PII in Remedy can only be accessed by authorized personnel using their individually assigned account credentials.

The Remedy application is physically secured and hosted in the CMS Baltimore data center. Physical controls, such as access control lists, CCTV monitoring, locked cages, and hardware redundancies are in place to protect the Remedy infrastructure. The network architecture conforms to CMS security requirements and logical access to this network is protected using firewalls and intrusion detection systems.