US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/06/2026

OPDIV:

CMS

Name:

Recovery Audit Contractor Data Warehouse

PIA Unique Identifier:

P-5912773-956516

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?

Existing

Does the system have Security Authorization (SA)?

Yes

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

Significant System Management Change

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

Recovery Audit Contractor Data Warehouse (RACDW) application has undergone a migration from the IT-CNP GovDataHosting Cloud Platform (GCP) Cloud Service Provider (CSP) to the CMS Hybrid Cloud environment. This migration includes changes to the physical server location, data storage processing, network configuration, and security measures/tools. Updates to the Technical architecture detail specific services utilized, data flow from the application to the CMS Hybrid Cloud. Personnel and roles have been adjusted to restrict access to authorized personnel via secure CMS connection. RACDW rehost change does not impact the collection, use, maintenance, or dissemination of PII/PHI. No application code changes, the type, format, and content of the PII collected and stored in the database are not modified during migration. The user interface and data entry points for PII remain the same, ensuring consistency on how PII is collected; existing business processes are retained. Security and Compliance Posture is Mapped: The existing security controls and compliance properties are largely maintained and mapped to new, but functionally equivalent,

cloud resources (e.g., moving from a physical firewall to a CMS security group with the same rules)

Describe the purpose of the system.

The Recovery Audit Contractors Data Warehouse (RACDW) is the data repository for all claims/line items reviewed by the Recovery Audit Contractors (RACs). It is a critical management/reporting tool for overseeing Fee-for-Service (FFS) RAC activity and tracking collections/reimbursements.

RACDW is used to track activities of the RACs, preventing interference with active program integrity and/or law enforcement investigations and ensuring that claims previously audited by other contractors are not reviewed again by the RACs. Centers for Medicare and Medicaid Services (CMS) uses the system to monitor RAC audits while ensuring that the RACs do not select claims that are exempt from review for various reasons, or where the providers are currently under investigation by program integrity and/or law enforcement entities. CMS also tracks RAC error findings via RACDW for the purpose of developing corrective actions.

RACDW will utilize a learning management system that hosts training modules for CMS personnel and contractors.

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

The RAC Data Warehouse collects selected claim elements (workload numbers, claim numbers, provider numbers, billing codes, amounts paid, and medical record notes) as well as the dates of various actions taken on those claims. Those selected claim elements are collected from the Recovery Audit Contractors, claim processing contractors and various program integrity/law enforcement entities for the purpose of monitoring RAC activity and preventing interference with fraud control activities.

Social security numbers are not required but may be transmitted to RACDW as part of the patient's medical records. SSN was historically a part of Health Insurance Claim Number (HICN) number identifying the beneficiary, however CMS is transitioning to using Medicare Beneficiary Identifier instead of HICN, and so only older claims will have SSN.

In addition to collecting selected claim elements described above, RACDW collects selected data elements that identify system users (all RACDW users are CMS employees, CMS contractors, or employees of other federal agencies). These elements include user first and last names, user ids and passwords, emails, and phone numbers. While these elements are PII, they are collected exclusively from RACDW users to control system access.

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

The RACDW performs numerous coordination, tracking, and reporting functions related to the collection of funds owed to CMS including the following; 1) enabling RACs to reflect progress with overpayment, underpayment and reversals identification and collection or payment of funds, 2) flagging claims and line items that have been previously medically reviewed, settled, or are under investigation currently by other entities so that the RACs do not duplicate the review effort, and 3) support monitoring and tracking the review process of a specific claim/line item.

Social security numbers are not required but may be transmitted to RACDW as part of the patient's medical records. SSN was historically a part of Health Insurance Claim Number (HICN) number identifying the beneficiary, however CMS is transitioning to using Medicare Beneficiary Identifier instead of HICN, and so only older claims will have SSN.

To serve the business functions described above, RACDW collects selected claim elements (workload numbers, claim numbers, provider numbers, billing codes, amounts paid, and medical record notes) as well as the dates of various actions taken on those claims. RACDW collects PII/PHI

for Medicare beneficiaries and will house more detailed medical records for some individuals. To control system access, RACDW does collect PII about its users (user ids, passwords, first and last names, emails, and phones). All RACDW users are CMS employees, CMS contractors, or employees of other federal agencies.

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
Medical Records Number
Medical Notes
Taxpayer ID
Other: User ID, and password

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

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

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

PII is used to identify RACDW users and to enable communication between RACDW system and administrative personnel and users (via email and phone). PII is also used to facilitate medical review audits and to provide auditors with access to medical records used for review outcome determinations.

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

n/a

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

U.S.C 301 Departmental Regulations is the legal authority for collecting user credentials.

Sections 1816 and 1874, 1874a, and 1875 of Title XVIII of the Social Security Act 42 US Code U.S. C1395H, 1395KK, and 1395II

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Online
Government Sources
Within OpDiv

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.

Whenever a user requires access, the user must fill out CMS user access request form which notifies the user that their personal information (name, email, and phone number) is being collected. Prior to submitting their user access request form to the RACDW administrator, the users must establish an account in CMS Enterprise User Administration (EUA) system, since their EUA IDs become the user ID's in RACDW.

RACDW does not interact with Medicare beneficiaries directly as part of the contract. The Medicare beneficiaries have no option to opt out of collection or use of their PII, since their claims have already been processed by Medicare and are stored in the National Claims History (NCH) data store. The system is not the authoritative source of the PII and does not modify any PII coming from NCH data store.

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 process for individuals to opt-out of the collection or use of their PII is defined on the CMS access request form that all users are required to complete prior to gaining access to the system. Opting out results in denial of access to the system.

RACDW does not interact with Medicare beneficiaries directly as part of the contract. The Medicare beneficiaries have no option to opt out of collection or use of their PII, since their claims have already been processed by Medicare and are stored in the National Claims History (NCH) data store. The system is not the authoritative source of the PII and does not modify any PII coming from NCH data store.

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

The users' PII collected in RACDW is used strictly to control user access, and changes to this data use or disclosure of this data are not anticipated. However, RACDW posts all necessary change notices for users when they access the system, which the users must acknowledge. In addition, since the users must establish an account in CMS EUA system prior to requesting an account in RACDW, any changes to CMS requirements impacting the use of their PII will be communicated to them by EUA.

RACDW does not interact with Medicare beneficiaries directly as part of the contract. The Medicare beneficiaries have no option to opt out of collection or use of their PII, since their claims have already been processed by Medicare and are stored in the National Claims History (NCH) data store. The system is not the authoritative source of the PII and does not modify any PII coming from NCH data store.

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 users themselves are the only source of that information which they provide by filling out the CMS user access request form. If the users have a concern about inappropriate source, usage, or disclosure of the PII information, they are to notify a CMS representative, who will investigate the concern and address it. The CMS representative can also request RACDW system administrator to update the user's credentials in the system if the user reports inaccuracies.

RACDW does not interact with Medicare beneficiaries directly as part of the contract. The Medicare beneficiaries have no option to opt out of collection or use of their PII, since their claims have already been processed by Medicare and are stored in the National Claims History (NCH) data store. The system is not the authoritative source of the PII and does not modify any PII coming from NCH data store.

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

PII in RACDW can only be entered, modified (or even viewed) via system user interface (which only the administrative users have access to). That interface collects audit trail for all activities- the system records who made which change and when. This audit trail is also available (in read only mode) to RACDW administrators via administrative interface – the presences of the audit trail for all PII additions or changes ensure non-repudiation. The audit trail would also help to restore the user PII in case of inadvertent corruption – if a RACDW user administrator overwrites the PII incorrectly by mistake, the older correct values are still available in the audit trail. The system user interface used by RACDW administrators to enter PII has validation rules in place that prevent incomplete data from being entered – all required data elements (user id, name, email, phone) must be present to create user accounts and they must have valid format and only relevant data elements can be entered. Since PII (user ids and emails) is used to authenticate users, the availability and accuracy of that information is ensured every time users successfully login – without this information being available and accurate in RACDW the users won't be able to access the system. In addition, to the system controls listed above, CMS security officer for RACDW conducts an annual review of all user accounts stored in RACDW in accordance with CMS requirements. As part of the audits, the integrity, accuracy and correctness of PII information associated with the user accounts is validated, as well as the relevancy of the PII and the need for continuing access to the users.

The beneficiaries' medical records, and associated PII, come into RACDW from medical review contractors over secure CMS network. Medical review contractors, in turn, receive them from providers in response to documentation requests triggered by audits. RACDW does not interact with Medicare beneficiaries directly as part of the contract. The Medicare beneficiaries have no option to opt out of collection or use of their PII, since their claims have already been processed by Medicare and are stored in the National Claims History (NCH) data store. The system is not the authoritative source of the PII and does not modify any PII coming from NCH data store. All medical records are securely stored in RACDW in encrypted format, and no change to the medical record files is possible through the system. The audit trail is kept for all medical records receipts and user downloads. The integrity, accuracy, and correctness of PII information associated with the medical records is assured since the documents come directly from medical service providers in read-only file format and are not modifiable.

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.

Based on CMS RACDW COR approval, RACDW administrators are granted access to the information system. Only RACDW administrators can access PII. RACDW system has a role-based access control process in place to determine who may access the system and what privileges are assigned to accomplish tasks required by their job. Role-based access control is used to ensure that only users with appropriate permissions (user account administrators) can access screens that allow to view, enter, and modify user account information (which is the only PII in the system).

Only users approved by management are authorized to access RACDW.

CMS program personnel control the access of medical review contractors to medical record files. That access is always read-only (users can only download the files, there is no way to modify them, since they are read-only) and is controlled by permissions set by CMS program personnel.

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 only PII in the system is user account information (user id, name, email, and phone) and medical record files for medical reviews that are tracked in the system. Only user account administrators have access to user account information, and this data set is the minimal amount of information necessary for user administrator to perform their job. Other system (non-administrative) users have no access to users' PII at all, as it is not relevant to their job functions.
Medical record files may contain patients' social security numbers, dates of birth, names, addresses, and medical notes, as well as providers' addresses and tax ids. However, only authorized medical review users have access to download medical record files, and that access is limited by line of business (role-based) so that each review contractor and auditor will only have access to medical records associated with their claims under review by their jurisdiction.

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.

RACDW User-Account Administrators receive the following CMS training:

Initial CMS Information Security & Privacy Computer Based Training (CBT)

Mandatory annual Security & Privacy Awareness Computer Based Training (CBT)

Annual Social Networking Training

Annual Phishing Awareness Training

Annual IT Security and Awareness Training

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

Annual Security Awareness Training

Annual Privacy Awareness Training

Annual Role-Based Security Training

Annual Disaster Recovery Tabletop Test

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.

RACDW follows the CMS Records Schedule, Section III. Medicare – Program Related which cites the National Archives and Records Administration (NARA) request for records disposition authority records schedule. Disposition Authority Number DAA-General Records Schedules (GRS)-2013-0006-0003, Section 3.1 denotes user identification records generated according to preset requirements, typically system generated. GRS or Superseded Authority N1- GRS-95-2 item 1c Citation, records are destroyed when business use ceases.

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

The RAC Data Warehouse is physically located at the Federal Information Security Management Act (FISMA) compliant data center within the CMS Hybrid Amazon Web Services (AWS) Cloud. Only authorized personnel have access to the data center, and all visitors are badged and escorted. Administration of PII at rest and in transit is in accordance with Federal Information Processing Standards (FIPS) 140-2 encryption standards and guidelines issued by the National Institute of Standards and Technology (NIST) pursuant to provisions of the Federal Information Security Management Act (FISMA) of 2002. The PII is administered in compliance with CMS security requirements, and only authorized system administrators and medical review contractors have access to PII data. Moreover, the system retains permanent audit trail of all activities involving PII data, so that for every instance of PII being edited or downloaded, it is known who made the edits (when, and what exactly changed), and who requested the download (and when).

Note: web address is a hyperlink.