US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/08/2025

OPDIV:

CMS

Name:

Risk Adjustment Data

PIA Unique Identifier:

P-3241952-687882

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

Significant System Management Change

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

No changes to physical location or PII/PHI elements.

Describe the purpose of the system.

The Risk Adjustment Data (RAD) system is a suite of data analysis and validation tools and functionalities instantiated by the Division of Encounter Data Risk Adjustment Operations (DEDRAO) Medicare Plan Payment Group (MPPG). The RAD has a current Authority to Operate (ATO) at a FISMA Moderate impact level. The system resides wholly within the CMS Cloud Hosting Facility (CHF) known as “CMS Hybrid Cloud” which is maintained by CMS Office of Information Technology (OIT).

The RAD system is comprised of two major components. The first, known as the RAD Tool application, is a web-based longitudinal validation and analytic tool and data repository instantiated

by the DEDRAO, specifically within MPPG.

The second component, known as the RAD Data environment, is a data processing infrastructure environment with no traditional front-end user interface. This environment supports data analysis, the Independent Verification and Validation (IV&V) of risk scores/model runs, payments (Monthly Membership Report (MMR)), plan reporting (MAO-004 and Model Output Reports (MOR)), and CMMI data analysis. It also supports the creation of Long-Term Institutional (LTI) Flags which are critical to payment calculations, and the creation of the Adjusted MMR which are critical to CMS analytic and modeling tasks. The RAD Data environment also supports the production of ad hoc analysis and data files in response to CMS requests. Future releases will support Beneficiary Payment Validation (BPV), and model development under the Medicare Part C [Medicare Advantage (MA)] and Part D (Medicare Drug) programs. The RAD Data environment of the RAD System is a modernization of data creation and validation processes that previously occurred within the CMS Mainframe.

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

RAD facilitates the independent creation and validation of the reports and data elements used by CMS for Risk Adjustment, some of which are transferred electronically to Medicare Advantage (MA) plans and Part D Sponsors. RAD does not share any data directly with MA or Part D plans. The system has built-in reporting, validation, and analytic capabilities. RAD processes data based on a predetermined schedule for certain tasks, and on an ad hoc basis as requested from CMS. Data is ingested from other CMS source systems for processing, namely the Integrated Data Repository (IDR), the Risk Adjustment Suite of Systems (RASS), the Internet Quality Improvement and Evaluation System (iQIES), Beneficiary Information in the Cloud (BIC), the Health Plan Management System (HPMS), and Medicare Advantage Prescription Drugs (MARx). The data sets include various CMS functions such as payment validation, risk score creation, risk score validation, and payment monitoring under the Medicare Part C [Medicare Advantage (MA)] and Part D (Medicare Drug) programs. The RAD operates with a ten-year retention schedule policy for all data.

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

The RAD System has a current Authority to Operate (ATO) at a FISMA Moderate impact level. RAD is a dual-function system. The first, known as the RAD Tool, is a web-based longitudinal validation and analytic tool and data repository instantiated by the Division of Encounter Data Risk Adjustment Operations (DEDRAO) Medicare Plan Payment Group (MPPG).

The second component is a data processing infrastructure environment with no traditional front-end user interface. This environment supports data analysis, risk score validation, and monitoring for payments under the Medicare Part C [Medicare Advantage (MA)] and Part D (Medicare Drug) programs.

The RAD Tool provides a mechanism for users to longitudinally review validation results and summary statistics and to respond to requests from Medicare Advantage Organizations (MAOs) regarding issues with their MAO-004 Reports [500-byte flat files, used by CMS to inform Medicare Advantage Organizations (MAOs) of the risk adjustment eligibility of diagnosis data submitted on accepted Encounter Data Records (EDRs)]. To access the RAD System, CMS employees and contractors must possess an Enterprise User Administration (EUA) ID and appropriate EUA job codes assigned to that ID. System authentication will be through EUA ID and password, and a single sign-on (SSO) Okta multi-factor authentication (MFA). The RAD data processing infrastructure requires CMS Cloud VPN access, in addition CMS employees and contractors must possess an Enterprise User Administration (EUA) ID and appropriate EUA job codes assigned to that ID. The data processing component uses the data ingested from other CMS source systems for processing, namely the Integrated Data Repository (IDR), the Risk Adjustment Suite of Systems (RASS), the Internet Quality Improvement and Evaluation System (iQIES), Beneficiary Information in the Cloud (BIC), the Health Plan Management System (HPMS), and Medicare Advantage Prescription Drugs (MARx) to provide predetermined and scheduled products, including independent verification and validation of production outcome created by a given CMS System of Record. In addition, the system

will ingest and store the production product to perform the comparison against. RAD will ingest source data such as Claims data, and beneficiary data (bene diagnoses/demographic data) to independently create files. Those data elements are also used for various Risk Adjustment model development, and Ad Hoc data analysis tasks. PII data elements such as social security number, name, date of birth, mailing address, date of death, health plan beneficiary numbers, and sex are maintained and stored in the RAD system. These data elements are necessary to complete critical tasks in the RAD system. As an example, for the validation of the MAO-004 report, data is typically processed monthly, according to the MAO-004 report generation schedule. Data are also updated on an ad hoc basis when CMS requires an off-schedule quality assurance validation. Source data is pulled from the IDR via a SQL query as a Parquet file, to independently create the MAO-004 report, which is compared against the RASS generated production version of that report. The RASS generated file is retrieved from a Simple Storage Service (S3) bucket maintained by that system, it is created as a Parquet file. Most data files produced and maintained in RAD are stored as Parquet files in an S3 bucket, except for summary level files that are maintained in a PostgreSQL RDS in the RAD Tool for reporting and information sharing purposes. Other outputs from RAD are created as Parquet and structured flat files or comma-separated values (CSV) files and downloaded locally for delivery to CMS. Data flow for other tasks follows a similar workflow.

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
Mailing Address
Other: Health plan beneficiary numbers, Sex, Date of Death, user credentials, Date of Death

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

Patients
Entitled Medicare Beneficiaries

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

RAD facilitates the independent creation and validation of the reports and data elements used by CMS for Risk Adjustment, some of which are transferred electronically to MA plans and Part D Sponsors. The system has built-in reporting, validation, and analytic capabilities. The data sets include various CMS functions, payment validation, risk score creation, risk score validation, and payment monitoring under the Medicare Part C [Medicare Advantage (MA)] and Part D (Medicare Drug) programs.

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

Secondary uses include using PII to research and perform various ad-hoc analytic tasks.

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

5 U.S.C Section 301 Departmental Regulations

Sections 1853(a)(3) and 1860D-15(c) and 15(e) of the Social Security Act (42 U.S.C. §§ 1395w-23,1395w-115);

Title 42 C.F.R. §§ 422.304, 422.308, 422.310,422.312 and 423.329.

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.

CMS Risk Adjustment Suite of Systems (RASS) - 09-70-0508

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OPDIV

Other HHS OPDIV

Identify the OMB information collection approval number and expiration date

RAD system Entities not collect PII or PHI from individuals. The RAD System utilizes data collected by CMS under OMB information collection approval number as follows: 0938-0878 expires 07/31/2026.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

The following agreements are in place that authorize the information sharing disclosure: Information Sharing Agreement (ISA), Data Use Agreement (DUA), and Memorandum of Understanding (MOU).

Describe the procedures for accounting for disclosures.

RAD adheres to the CMS Computer Security Incident Response program and HHS directives. Whenever a security breach is suspected or detected, the appropriate parties (CMS and/or CMS contractors) are notified. Then the CMS IT Service Desk and CISO are both notified with information detailing breach and a Request is opened to conduct investigation into situation. If necessary, the RAD ISSO and/or business owner will take further action according to severity of if recommended by CMS CISO. For all data disclosures, requestors asking for from must complete a DUA which tracks who disclosure was with, reason as well date disclosure.

RAD is not a SOR (System of Record) and essentially inherits data from other systems i.e. the Risk Adjustment Suite of Systems (RASS), the Encounter Data Processing System (EDPS), and the Internet Quality Improvement and Evaluation System (iQIES)]. Each system is covered by its own PIA and each system has its own system documentation and requires that a Data Use Agreement (DUA) be in place to document and track those disclosures before sharing data with other organizations.

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

Prior to coming to this system, the process to notify individuals that their personal information will be collected occurs at the provider level at the time of services rendered. RAD is not a public facing system and the data therein is only accessible within the boundaries of CMS systems and networks. The source data for the RAD system comes from other CMS systems which are Systems of Record

(SOR) for the data: [Integrated Data Repository (IDR), the Risk Adjustment Suite of Systems (RASS), and the Internet Quality Improvement and Evaluation System (iQIES)]. Each system is covered by its own PIA, and it is the responsibility of each source system to provide notification of collection.

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.

This system does not require submission of PII by individuals.

The source data for the RAD system comes from other CMS systems which are Systems of Record (SOR) for the data: [Integrated Data Repository (IDR), the Risk Adjustment Suite of Systems (RASS), and the Internet Quality Improvement and Evaluation System (iQIES)]. Each system is covered by its own PIA and it is the responsibility of each source system to provide individuals the option to opt-out.

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

Participation in MA and MAPD plans is voluntary and requires an affirmative election to join. When an individual enrolls in a plan, as part of the application package, the beneficiary is required to sign the Agreement Page. Thus, Managed Medical Assistance (MMA) enrollment equates to beneficiary consent. The Privacy Act permits CMS to disclose information without an individual’s consent if the information is used to for a purpose that is compatible with the purpose(s) for which the information was collected. Any such disclosure of data is known as a “routine use.” CMS policy prohibits the release even of non-identifiable information, except pursuant to “routine use.” In terms of system changes, the CMS Business Owner and Information System Security Officer (ISSO) of RAD vets all contractor- proposed system changes and ensures that such changes fall within the Federal Information System Management Act (FISMA) security parameters of the system as well as within the scope of the System of Record (SOR) associated with it. As such, system modifications never include the direct collection of PII from individuals and never fall outside of the research purposes authorized by the system's associated SOR. RAD follows the CMS Enterprise User Authentication system guidelines and access to PII is given on a restricted need to know basis. An access review of users that have access to PII and their user-roles is performed every 90 days. The source data for the RAD system comes from other CMS systems which are Systems of Record (SOR) for the data: [Integrated Data Repository (IDR), the Risk Adjustment Suite of Systems (RASS), and the Internet Quality Improvement and Evaluation System (iQIES)]. Each system is covered by its own PIA, and it is the responsibility of each source system to provide individuals notification and consent of PII collection.

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 subject individual contacts the RAD system manager, and reasonably identifies the record and specifies the information to be contested. The contact states the corrective action sought and the reasons for the correction with supporting justification. These procedures are in accordance with department regulation 45 CFR 5b.7.

If an individual believed his or her PII had been inappropriately obtained, used, or disclosed or that his or her PII is inaccurate, the individual would contact the CMS IT Service Desk directly via email (CMS_IT_Service_Desk@cms.hhs.gov) or phone at 1-800-562-1963, and CMS would push the issue to all relevant internal organizations and contractors, including CMS staff responsible for taking in individuals' concerns about their PII.

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

Periodic review of PII data is performed during the annual RAD Security Control Assessment as well as during the annual Privacy Impact Assessment review. Reviews are also performed when data

within RAD falls outside the scope of the 10-year data retention schedule.

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.

RAD leverages CMS Enterprise User Authentication (EUA) as the primary method to create and restrict access to the system. Users must possess an EUA account in good standing, and then apply for the proper Job Codes for access to CMS Cloud Greenfield assets. Access is granted on a restricted need to know basis by the CMS Contracting Officer Representative (COR) for the RAD system. An access review of users that have access to PII and their user roles is performed every 90 days.

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.

Systems based within the CMS Cloud Greenfield Cloud Hosting Facility are subject to Role Based Access Control policy (RBAC) enforced by OIT. Access to an RBAC Role is granted by approval of the CMS COR. Within RBAC, a standardized set of user roles define permissions and policies granted to users within cloudtamer.io and therefore within their respective Amazon Web Services (AWS) environment(s). PII is restricted to certain of these AWS Environments.

Reviews of RBAC access by Organizational Users with access to PII contained within the RAD system authorization boundary (CMS and Contractor Personnel) are conducted quarterly.

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 users of the RAD system (which are limited strictly to CMS or CMS Contractor personnel) must possess an EUA ID to access the system. In order to maintain an EUA ID in good standing, all personnel must complete annual CMS Computer Based Training (CBT). In addition, CMS and Contractor personnel complete the annual HHS Records Management course. Contractor Personnel also complete mandatory contractor supplied annual General Security and Privacy Awareness training. Contractor records of completion are available upon request.

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

In addition to the previously mentioned generic security awareness training, selected RAD contractor personnel have Significant Security Responsibilities (SSR) as defined in NIST SP 800-181 - National Initiative for Cybersecurity Education (NICE), CMS IS2P2, and CMS Risk Management Handbook (RMH) Chapter 2. Personnel with SSR receive annual targeted training based upon the specific Knowledge, Skills, and Abilities (KSA) required for their particular job function.

The RAD team has determined that RAD personnel occupy the following significant security roles:
System Security Officer (SSO);
Developer/Programmer;
Application Security Tester;
Penetration Tester;
Database Administrator;
System Administrator;
Senior System Analyst.

All personnel who have been determined to have SSR are required to sign an affidavit acknowledging their roles and responsibilities, as well as the knowledge, skills, and abilities commensurate to their roles. Training mapped to KSAs specific to each SSR is provided on an annual basis.

Evaluation of SSR is performed on an annual basis to ensure compliance with NICE Framework objectives. Records of evaluation and individual compliance are maintained by the contractor for auditing purposes, and are available for examination by CMS or designated third-party assessors on a quarterly basis.

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.

HHS and CMS have policies and guidelines in place with regards to the retention and destruction of PII. RAD will adhere to the HHS and CMS policies for retention and destruction of data. RAD does internally have a data retention policy where PII/PHI data will be retained for 10 years. Records are maintained with identifiers per the CMS Master Security Plan for 10 years per National Archives and Records Administration (NARA). Where data with PII is subject to a litigation hold, it will be maintained in RAD until the hold is lifted. Any PII/PHI not subject to a litigation hold will be destroyed once it reaches the 10-year retention threshold.

Data in the RAD system falls under General Records Schedule Bucket 7 - DAA-0440-2015-0009 Sequence Number 1.2 Analytic and Research Files (restricted). Disposition of these records occurs via transfer to the National Archives for Accessioning 20 years after cutoff. The agency will transfer records destined for disposal annually.

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

The RAD system utilizes the Resource Access Control Facility (RACF) controls that are in place per the Enterprise User Administration (EUA) as far as technical and administrative electronic access to records. It also relies heavily upon CMS enterprise components to process transactions and authenticate users. Thus, RAD inherits the security controls in place for the CMS infrastructure that are contained in the Master Security Plan and CMS Data Center General Support System (GSS) System Security Plan (SSP) to support their external Business partners, enterprise file transfers and user authentications, and further inherits the security controls and guidelines for User and Data Assets, Physical architecture, Information and Data flows, MAO’s connectivity to CMS and external Business partners’ information sharing functions and separate security agreements. Technical Controls: RAD utilizes the RACF controls that are in place per the EUA as far as technical and administrative electronic access to records. RAD has implemented the CMS ARS controls and NIST 800-53 Security controls for a Moderate system for access control, auditing, and media protection of the RAD. Physical Controls: The RAD is maintained in the CMS AWS Cloud Greenfield Cloud Hosting Facility. Physical controls are inherited from AWS. The RAD system utilizes the Resource Access Control Facility (RACF) controls that are in place per the Enterprise User Administration (EUA) as far as technical and administrative electronic access to records. It also relies heavily upon CMS enterprise components to process transactions and authenticate users. Thus, RAD inherits the security controls in place for the CMS infrastructure that are contained in the Master Security Plan and CMS Data Center General Support System (GSS) System Security Plan (SSP) to support their external Business partners, enterprise file transfers and user authentications, and further inherits the security controls and guidelines for User and Data Assets, Physical architecture, Information and Data flows, MAO’s connectivity to CMS and external Business partners’ information sharing functions and separate security agreements. Technical Controls: RAD utilizes the RACF controls that are in place per the EUA as far as technical and administrative electronic access to records. RAD has implemented the CMS ARS controls and NIST 800-53 Security controls for a Moderate system for access control, auditing, and media protection of the RAD. Physical Controls: The RAD is

maintained in the CMS AWS Cloud Greenfield Cloud Hosting Facility. Physical controls are inherited from AWS.
Administrative Controls: Access to the RAD is granted through EUA job codes, which must be approved by CMS COR and First Approver. Systems based within the CMS Cloud Greenfield Cloud Hosting Facility are subject to Role Based Access Control policy (RBAC) enforced by OIT. Access to an RBAC Role is granted by approval of the CMS COR. Within RBAC, a standardized set of user roles define permissions and policies granted to users within cloudtamer.io (Kion) and therefore within their respective Amazon Web Services (AWS) environment(s). PII is restricted to certain of these AWS Environments. The administrative and user accounts for the RAD system are reviewed every 90 days.