US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/15/2017

OPDIV:

CMS

Name:

Risk Adjustment System-RAPS

PIA Unique Identifier:

P-2454792-079917

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

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

A Risk Adjustment Processing System (RAPS) User Interface (UI) has been implemented using Enterprise Microstrategy Reports. The UI has been established as a method of allowing the RAS/RAPS business owner to establish limits on which Medicare Advantage Organizations (MAO) can submit Risk Adjustment Processing System (RAPS) submissions to the system.
There are two roles established for the UI: Data- Entry End-User and Approver-End User. The Data-entry end-user can make entries to either open or close a submission window based on Health Plan Identification Number or by a specific Payment Year. The Approver End-User is responsible for approving entries made into the RAPS UI. There is no PII/PHI contained within the UI.

In addition, although still active, the Risk Adjustment System Analytic Reporting Tool and its capability is in the process of being migrated into the Integrated Data Repository (IDR). For this reason, there is no longer end-user access to the system, but for development and validation purposes, it is still being used to develop and transition reports and other information to the IDR.

Describe the purpose of the system.

The Risk Adjustment Suite of Systems (RASS) consists of the following systems the Risk Adjustment System (RAS) and the Risk Adjustment Processing System (RAPS).

The RAS serves two major business functions. The RAS performs the primary function to compute Risk Adjustment Factors (RAF) or RAF scores for each Medicare beneficiary using the regression models that were developed using Statistical Analysis Software (SAS). These scores are a relative weight of predicted health risks for each beneficiary based on their past medical history data. RAS receives the most current data for each beneficiary from three sources: RAPS, Master Beneficiary Database (MBD)'s Common Medicare Environment (CME), and National Medicare Utilization Database (NMUD) system. It processes data extracted from these three systems to compute the RAF scores. These scores are sent to the Medicare Advantage Rx (MARx) payment system, which determines the beneficiary level payments for the Medicare Advantage (MA) and Prescription Drug Plans (PDPs).

RAPS supports the RAS primary business function by receiving, processing, and storing Medicare Advantage Organization (MAO) risk adjustment claims data. MAOs submit beneficiary data through the Front-End Risk Adjustment System (FERAS) at the Palmetto GBA (contract name-not an acronym) Data Center. FERAS receives, stores, and transmits correctly formatted beneficiary data to RAS via RAPS.

A secondary business function is to provide information to CMS for reporting and analysis based on the data supplied by RAPS and the RAF scores computed by RAS. In addition to the risk adjustment factors, RASS receives and processes contract data and state and county lookup data from Health Plan Management System (HPMS), and the MARx Monthly Membership Detail Report (MMDR) payment data to use for analysis and reporting of Payment and Adjusted MMR data files.

The CME, NMUD, HPMS, and MARx systems are outside the boundary of RAS-RAPS and are covered by their own PIAs. FERAS is within the RAS-RAPS boundary and is covered by this PIA.

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

Risk Adjustment System/Risk Adjustment Processing System requires Medicare Advantage and Medicare Advantage Prescription Drug submitters to provide Health Insurance Claim Number (HICN), ICD-9-CM Diagnosis Code, Service from date, Service through date, Provider Type (Hospital Inpatient, Hospital Outpatient and Physician), Patient Control Number (optional) and Date of Birth (optional) for routine use. Submission of PII data is mandatory as a condition of payment.

The submitted data is necessary to comply with the Medicare Modernization Act payment provisions.

Risk Adjustment System downloads (as routine use) Personally Identifiable Information (PII) including HICN, Beneficiary Identification Code (BIC) and Beneficiary Name, as well as, non-PII program and system data from National Medicare Utilization Database, Medicare Beneficiary Database (MBD)/Common Medicare Environment and Health Plan Management System. The extracted or shared data is for routine use, and is necessary to comply with the Medicare Modernization Act payment provisions.

RAS uploads (as routine use) PII including Health Insurance Claim Number, Beneficiary Identification Code (BIC) and Beneficiary Name) and non-PII program and system data to Medicare Advantage Prescription Drug System. The shared data is for routine use, and is necessary to comply with the Medicare Modernization Act reporting and payment provisions.

Non-PII and system data refers to data that is pulled from the CME, NMUD, HPMS, and RAPS that involves any of the following:

Beneficiary Low Income Territory - Captures the Low Income Part D Enrollees who reside in the US Territories. Also captures the risk adjustment dates so that MARx can properly risk adjust the Part D payment to the plans in which the beneficiary is enrolled.

Beneficiary Medicare Advantage Prescription Drug (MAPD) Enrollment - Contains Medicare Beneficiary's delivery selections, MA, MA PDP or PDP, and coverage periods for the selection. Additionally other characteristics relevant to the selection are also captured. Both current and historical data are retained.

Beneficiary Medicare Advantage Medicaid Eligibility - Contains Medicaid Eligibility periods for a Medicare/Medicaid Beneficiary's enrolled in either Medicare Advantage Plans or Medicare Advantage Plans +PDP. Both historical and current information is captured.
Beneficiary Medicare Status - captures the combination of reasons why a beneficiary is entitled to Medicare (i.e. Disabled and End Stage Renal Disease (ESRD)).

Beneficiary Point Of Sale - A beneficiary who has been identified by the Point of Sale contractor as Medicaid eligible.

CME Part A Entitlement - contains periods of Part A entitlement for a Medicare Beneficiary.

Beneficiary Medicare Part B Entitlement - contains periods of Part B enrollment coverage for a Medicare Beneficiary.

RAS/RAPS follows the CMS Enterprise User Authentication (EUA) 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 180 days.

PII collected from users/system administrators in order to access the system, consists of user credentials (i.e. username, password, Personal Identity Verification (PIV) card and/or email address). Users system administrators include OpDiv employees and direct contractors (using HHS user credentials only).

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

The Risk Adjustment Suite of Systems (RASS) consists of the following systems the Risk Adjustment System (RAS) and the Risk Adjustment Processing System (RAPS).
The RAS serves two major business functions. The RAS performs the primary function to compute Risk Adjustment Factors (RAF) or RAF scores for each Medicare beneficiary using the regression models that were developed using Statistical Analysis Software (SAS). These scores are a relative weight of predicted health risks for each beneficiary based on their past medical history data. RAS receives the most current data for each beneficiary from three sources: RAPS, Common Medicare Environment (CME), and National Medicare Utilization Database (NMUD) system. It processes data extracted from these three systems to compute the RAF scores. These scores are then sent to the Medicare Advantage Rx (MARx) payment system, which determines the beneficiary level payments for the Medicare Advantage (MA) and Prescription Drug Plans (PDPs).

RAPS supports the RAS primary business function by receiving, processing, and storing Medicare Advantage Organization (MAO) risk adjustment claims data. MAOs submit beneficiary data through the Front-End Risk Adjustment System (FERAS) at the Palmetto GBA Data Center. FERAS receives, stores, and transmits correctly formatted beneficiary data to RAS via RAPS.

A secondary business function is to provide information to CMS for reporting and analysis based on the data supplied by RAPS and the RAF scores computed by RAS. In addition to the risk adjustment factors, RASS receives and processes contract data and state and county lookup data from HPMS, and the MARx Monthly Membership Detail Report (MMDR) payment data to use for analysis and reporting of Payment and Adjusted MMR data files.

Risk Adjustment System/Risk Adjustment Processing System requires Medicare Advantage and Medicare Advantage Prescription Drug submitters to provide Health Insurance Claim Number (HICN), ICD-9-CM Diagnosis Code, Service from date, Service through date, Provider Type (Hospital Inpatient, Hospital Outpatient and Physician), Patient Control Number (optional) and Date of Birth (optional) for routine use. Submission of PII data is required as a condition of payment. The submitted data is necessary to comply with the Medicare Modernization Act payment provisions.

Risk Adjustment System downloads (as routine use) Personally Identifiable Information (PII) including HICN, Beneficiary Identification Code (BIC) and Beneficiary Name, as well as, non-PII program and system data from National Medicare Utilization Database, Medicare Beneficiary Database/Common Medicare Environment and Health Plan Management System. The extracted or shared data is for routine use, and is necessary to comply with the Medicare Modernization Act payment provisions.

RAS uploads (as routine use) PII including Health Insurance Claim Number, Beneficiary Identification Code (BIC) and Beneficiary Name) and non-PII program and system data to Medicare Advantage Prescription Drug System. The shared data is for routine use, and is necessary to comply with the Medicare Modernization Act reporting and payment provisions.

RAPS performs edit/update functions on Medicare Advantage Organization (MAO) beneficiary diagnosis data input files daily. These input files are transmitted through FERAS to RAPS. RAPS performs edits on the input file data and then stores the data in the RAPS database. After the final edits are completed, RAPS transmits the return files and error reports to FERAS for distribution to the MAOs.

In order to receive access to the RAS-RAPS data, a user must have a CMS user ID as well as the appropriate RAS-RAPS job codes. RAS-RAPS is a batch system and therefore does not have a graphical user interface for viewing the data. The RAS-RAPS data is stored within the Integrated Data Repository (IDR) and a user must request access to this system as well in order to view it. All user IDs and job code requests

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

Yes

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

Date of Birth

Name

E-Mail Address

Other - HICN; BIC; ICD-9-CM Diagnosis Code, Service from date, Service through date, Provider

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

Employees

Vendor/Suppliers/Contractors

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?

RAPS: receives PII, health and other claims data (via the Front End Risk Adjustment System (FERAS), which formats the initial data) from Medicare Advantage (MA) and Medicare Advantage Prescription Drug (MAPD) organizations, submits the formatted data to RAS, and returns submission reports to the submitters. The collection is required to generate health risk scores for MA and MAPD enrolled Medicare beneficiaries.

National Medicare Utilization Database (NMUD): provides FFS PII, health and other claims data. This collection is required to generate health risk scores for all Medicare beneficiaries.

MBD/Common Medicare Environment (CME): provides PII and beneficiaries demographic data. This collection is required to generate health risk scores for Medicare beneficiaries.

Health Plan Management System (HPMS): provides the most current and accurate Contract and Plan level data. This data feed enables RAS to summarize and stratify Contract and Plan data. This collection is required to generate reports, which are used to track and monitor the performance of Medicare Advantage Organizations (MAOs). As mentioned in the response to question 10, the Risk Adjustment System Analytic Reporting Tool and its capability is in the process of being migrated into the Integrated Data Repository (IDR). For this reason, there is no longer end- user access to the system, but for development and validation purposes, it is still being used to develop and transition reports and other information to the IDR.

Medicare Advantage Prescription Drug System (MARx): receives PII, RAFs and other data from RAS, and provides the data outcomes to MAOs. This collection is required to generate MA payments and reports at and on the Medicare beneficiary level.

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

The secondary uses include using PII/PHI for validation and testing of the three RAS Model Runs (initial, mid-year, and final) and is also used for research and analytic purposes by CMS and other Federal agencies. There is currently a high finding for RAS/RAPS for using sensitive data in the validation and development environments. The current status is that meetings and discussions have been held between CMS components to come up with a solution for this high finding which includes RAS/RAPS and other MAPD systems. There is no current timeline and it is unsure when a solution will be implemented.

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

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.

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

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Other Federal Entities

Identify the OMB information collection approval number and expiration date

0938-0878 expires 03/31/2020

Is the PII shared with other organizations?

Yes

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

Other Federal Agencies

The information is shared with other federal agencies such as Department of Justice (DOJ), Government Accountability Office (GAO), Office of the Inspector General (OIG). This shared for data analytics, research and periodic and annual audits performed by such agencies. Users can access the data via the CMS Mainframe and IDR.

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

The following agreements are in place that authorizes the information sharing disclosure: Information Sharing Agreement (ISA), Data Use Agreement (DUA), and Non-Disclosure agreements.

Describe the procedures for accounting for disclosures.

RAS/RAPS 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 CMS CISO are both notified with information detailing the breach and an IT Service Request is opened to conduct an investigation into the situation. If necessary, the RAS/RAPS ISSO and/or business owner will take further action according to the severity of the breach if recommended by the CMS IT Service Desk or CMS CISO. For all data disclosures, requestors asking for data and information from the RAS/RAPS must complete a CMS DUA which tracks who the disclosure was with, the reason for the disclosure as well as the date of the disclosure.

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. RAS-RAPS is not a public facing system and the data therein is only accessible within the boundaries of CMS systems and networks.

In order to receive access to the RAS-RAPS data, a user must have a CMS user ID as well as the appropriate RAS-RAPS job codes. RAS- RAPS is a batch system and therefore does not have a graphical user interface for viewing the data. The RAS-RAPS data is stored within the Integrated Data Repository (IDR) and a user must request access to this system as well in order to view it. All user IDs and job code requests must follow the CMS Enterprise User Access (EUA) rules and guidelines and be approved by the RAS-RAPS business owner.

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.

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, Medicare Modernization Act (MMA) enrollment equates to beneficiary consent. The Privacy Act permits CMS to disclose information without an individual's consent if the information is used 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."

RAPS (via FERAS) receives PII and non-PII beneficiary health claims data from MA and MAPD plans, and discloses PII and non-PII beneficiary data to external and internal sources pursuant to determining beneficiary payment rates (i.e., pursuant to routine use).

RAS receives and discloses PII and non-PII beneficiary data from and to internal sources (i.e., RAPS, MBD/CME, HPMS, NMUD and
MARx pursuant to determining beneficiary payment rates and plan performance, in the case of RAS ART (i.e., pursuant to routine use). External sources include other federal agencies such as GAO, DOJ, and OIG and other CMS contractors such as IBM, Palmetto GBA, Fu, RTI, and SAS.

RAS/RAPS 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 180 days.

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, 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 RAS/RAPS 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.

RAS/RAPS 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 180 days.

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 RAS/RAPS 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 CMS directly, 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.

RAS/RAPS 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 180 days.

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 RAS/RAPS Security Control Assessment as well as during the annual Privacy Impact Assessment review. Reviews are also performed when data within RAS/RAPS falls outside the scope of the 10 year data retention schedule.

RAS/RAPS 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 180 days.

The PII data within the RAS/RAPS are protected by the CMS EUA/Resource Access Control Facility (RACF) guidelines and permissions and only production job IDs have the authority to update PII data in the RAS/RAPS applications. RAS/RAPS is a batch application and RAS/RAPS does not have a User Interface that allows change of the PII data. Users are trained during on-boarding and annually thereafter on HHS CMS Information security policy and re-certification program; background checks prior to system access; and additional IBM policies and HIPAA training on security standards for handling, disclosure, and destruction of confidential or sensitive regulated data.

Since RAS/RAPS is a batch system, the PII data is only available on the CMS mainframe. This PII data can be extracted to a mainframe file and made available only on the mainframe. RAS/RAPS uses all current PII data, from various sources, in all system processes for the purposes needed of Risk Adjustment. All unnecessary, irrelevant, incoherent, and inaccurate PII is removed from the system when a data file is found to be incorrect or corrupted by application processes and model re-runs that replace the original batch file.

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

Users:

CMS internal staff uses RAS/ RAPS to utilize beneficiary data in developing the health risk factors to be used for payment, to analyze the performance of plans and to address the concerns of MAOs.

Administrators:

Required to support administration activities, interactions of internal users and external interfacing activities.

Developers:

Required to maintain, test, validate and support health risk factor development and MAOs.

Contractors:

Required to maintain, test, validate and support health risk factor development and MAOs. These contractors are direct contractors. Direct contractors are contractors that operate on behalf of the agency and use the agency's credentials when doing so.

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

RAS/RAPS 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 180 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.

RAS/RAPS follows the CMS EUA 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 180 days. RAS/RAPS data has job codes associated with specified user roles and access levels for RAS/RAPS and the IDR. Based on a user role, the user is granted access to only the data within the view requested. If more detailed information is requested, then a justification for the needed data is requested as well.

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.

In order to access RAS/RAPS data, a CMS User ID is required. In order to receive a CMS User ID, a user must complete the mandatory CMS Computer Based Training and Privacy Training after initial user ID creation and also on an annual basis thereafter to retain CMS system access. This annual training is required by CMS and the CMS Chief Information Security Officer (CISO) and is mandatory for all CMS Users.

In addition to the CMS Security Awareness and Privacy Act training, during the on-boarding process and annually thereafter, all IBM RASS contractor employees are required to complete the following privacy related training, which covers Privacy Act requirements and related security requirements. These courses emphasize the CMS requirements for the protection of the confidentiality and integrity of personally identifiable information (PII) and protected health information.

IBM Data Security & Privacy Training IBM HIPAA Overview
IBM HIPAA Compliance Guide IBM HIPAA Compliance Program

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

None

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 do have policies and guidelines in place with regards to the retention and destruction of PII. RAS/RAPS will adhere to the HHS and CMS policies for retention and destruction of data. RAS/RAPS does 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). Per DAA-GRS- 2013-0006-0003, Destroy 1 year(s) after user account is terminated or password is altered or when no longer needed for investigative or security purposes, whichever is appropriate.

RAS/RAPS is also included in the CMS Records Schedule under XIV. Electronic System, Section T - Medicare Advantage and Rx Plan Operations (MARPO). According to the CMS records schedule, data are deleted when they have been entered into the Master Files or database and verified, or when no longer required to support reconstruction of, or serves as a backup to, a master file or database, whichever is later. Please refer to pages 116- 117 of the referenced document below for more clarification.

http://intranet.cms.gov/Component/OSORA/IRIS G/DRIS/RM/Downloads/CMS-Records- Schedule-E13.pdf

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

All of the RAS applications (i.e., RAS, RAPS and RAS ART) utilize the RACF controls that are in place per the Enterprise User Administration (EUA) as far as technical and administrative electronic access to records. They also rely heavily upon CMS enterprise components to process their transactions and authenticate users. Thus, RAS/RAPS 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:
RAS/RAPS inherits controls from the CMS Baltimore Data Center and utilizes the RACF controls that are in place per the EUA as far as technical and administrative electronic access to records. RAS/RAPS has implemented the CMS ARS controls and 800-53 Security controls for a Moderate system for access control, auditing, and media protection of the RAS/RAPS.

Physical Controls:
The RASS is maintained in the CMS Baltimore Datacenter that has strict physical security controls in place including: guards, mantraps, surveillance/closed circuit TV, and key cards. Access to the RASS is strictly monitored from a physical perspective.

Administrative Controls:
Access to the RASS is granted through EUA job code based role access and is based on CMS Government Task Lead (GTL) and ISSO approval along with RASS PM approval. The administrative and user accounts for the RASS system are reviewed every 180 days.