US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/27/2025

OPDIV:

CMS

Name:

CCIIO Customer Relations Management System

PIA Unique Identifier:

P-5882866-285645

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?

Yes

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.

Other: Addition of Independent Dispute Resolution (IDR) Technical Assistance (TA) Business Rule Engine (IDR TA RE) into authorization boundary

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

1. The Independent Dispute Resolution Technical Assistance Rules Engine (IDR TA RE) is incorporated into the CCRMS authentication boundary.

2. Own (previously 'OwnBackup'), a Salesforce Data backup solution was implemented

3. Marketplace Assister Technical Support (MATS) was renamed to Federal Services System Support and Oversight (FSSSO).

Describe the purpose of the system.

The CCIIO Customer Relations Management System (CCRMS) was created to support Affordable Care Act (ACA) back-office and customer service initiatives. CCRMS spans two CCIIO programs—Consumer Support Group’s (CSG) Federal Services System Support and Oversight (FSSSO)

program and Payment Policy and Financial Management Group's (PPFMG) Premium Stabilization Programs and Marketplace Operational Support (PSPMOS or PSP) program. Under each program, there are Salesforce orgs for CCIIO:

The Salesforce Software-as-a-Service (SaaS) organizations are:

PSP-RARI
Risk Adjustment and Re-Insurance (RARI)/ Risk Adjustment Data Validation (RADV)/Vendor Management (VM): The system receives and processes inquiries from organizations that participate in the Marketplace. It brings together the processes of intaking and responding to questions, hosting a library with program information, and intaking and completing audit processes.

Federal Services System Support & Oversight
(FSSSO) MATS: The system collects and processes inquiries from Marketplace Assisters and organization that support to consumers in completion, enrollment, and eligibility assistance.
Independent Dispute Resolution (IDR): The IDR is a module within MATS org that establishes an independent pathway for issuers, providers, and consumers to settle payment disputes, providing information on payment practices to inform future policymaking, establish an effective IDR entity (IDRE) certification process that ensures IDR parties have easy access to qualified and carefully evaluated federal IDREs to help successfully resolve their IDR case.
Independent Dispute Resolution - Technical Assistance (IDR TA) Rules Engine (RE) – The IDR TA Rules Engine, managed by Index Analytics automate the review of disputes in the IDR TA queue and increase the efficiency and consistency of the eligibility recommendations. The RE will manage:
Complaints: Complaints is an established process to receive issuer and provider complaints of violations of No Surprise Act rules, including non-compliance with out-of-network service billing (payer is billed by provider and doesn't think they should be), and non-payment by payer to provider (provider submits complaint against payer).

System Plan and Issuer Data Reporting (SPIDR): SPIDR is a platform that provides automation to facilitate continuous process improvement to support the highly complex operations related to the design, display, certification, and management of qualified health plans. It collects, evaluates, and certifies Quality Health Plans (QHPs) from Issuers; and allows users to access their Issuer/Plans and Case information configured to meet the CCIIO needs for managing and reporting on Issuer and Plan Management activities.

IDR TA BRE
As part of the No Surprises Billing Act, the IDR TA team is developing the IDR TA Rules Engine (RE) Minimum Viable Product (MVP), to automate the review of disputes in the IDR TA queue and increase the efficiency and consistency of the eligibility recommendations. RE aims to process bulk disputes using eligibility criteria defined in the CMS approved Standard Operating Procedures (SOPs) to review dispute eligibility and reduce the IDR TA backlog as quickly as possible. RE will expand the current flagging system to further categorize and flag dispute details to provide indicators of the potential for ineligibility, the dispute complexity, and the number of documents likely to be required. RE leverages artificial intelligence (AI) models to identify the presence or absence of necessary data points within documentation. RE will feed outputs of prior steps along with IDR Salesforce Portal data to guide the analyst to the shortest pathway to determine eligibility and produce outputs of standardized outreach or eligibility determination language.

AWS

RADV, EZ-Protect (anti-virus solution) for Salesforce file attachments, and Microlearning courseware files are maintained in the AWS environment.

¿CCRMS utilizes the AWS se

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

CCRMS:

CCRMS collects, maintains, and stores information at multiple levels:

- Pertaining to individual and company names, email addresses, phone numbers, mailing addresses, taxpayer identification numbers, date of birth, medical record number, medical notes, financial account information and social security numbers.
- User ID, Enrollment accounts, payment information, Issuer EDGE enrollment and claim data (this is not maintained at the enrollee level).
- Department of Health and Human Services (HHS) RADV Sampling Reports limited individual enrollee claim and medical record data.

IDR TA RE

The IDR TA RE will access the following IDR Salesforce Portal Fields: IDR_TA_Status, IDR_TA_Recommedation, IDR_TA_Recommendation_Comment, IDR_TA_Dispute_Flags through daily data refreshes from the IDR Salesforce Portal. The IDR TA RE returns analytical data to existing data fields in the IDR Salesforce through an IDR Salesforce API.

The IDR TA RE AI model will access dispute resolution data from existing AWS S3 buckets periodically to train the AI model for accuracy. The dispute resolution data accessed by the AI model for training/accuracy does contain PII/PHI fields of information: Name, Dispute Number, Claim Number, Service Code, and Date of Service.

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

CCRMS

Risk Adjustment and Re-Insurance (RARI)/ Risk Adjustment Data Validation (RADV)/Vendor Management (VM): The system receives and processes inquiries from organizations that participate in the Marketplace. It brings together the processes of intaking and responding to questions, hosting a library with program information, and intaking and completing audit processes. Data is stored back to the system inception, which is nine (9) years.

(FSSSO) MATS: The system collects and processes inquiries from Marketplace Assisters and organizations that support consumers in completion, enrollment, and eligibility assistance.

Complaints: Complaints are an established process to receive issuer and provider complaints of violations of No Surprise Act rules, including non-compliance with out-of-network service billing (payer is billed by provider and doesn't think they should be), and non-payment by payer to provider (provider submits complaint against payer).

System Plan and Issuer Data Reporting (SPIDR): SPIDR is a platform that provides automation to facilitate continuous process improvement to support the highly complex operations related to the design, display, certification, and management of qualified health plans. It collects, evaluates, and certifies Quality Health Plans (QHPs) from Issuers; and allows users to access their Issuer/Plans and Case information configured to meet the CCIIO needs for managing and reporting on Issuer and Plan Management activities.

MATS data goes back to the system inception, which is eight (8) years, and the SPIDR has five (5) years of data stored.

IDR TA RE

The IDR TA RE will access several existing fields in the IDR Salesforce Portal, IDR TA Work object will be updated based on the Rules Engine output. The values will be passed in the Rules Engine Utility API payload. This information is not stored or shared.
The IDR TA RE AI model will periodically access existing dispute resolution information from existing, persistent, and encrypted S3 buckets that contain PII/PHI (listed above). The dispute resolution fields that contain PII/PHI are temporarily accessed, not stored persistently, for purposes of training the AI model and are not shared.

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
Financial Accounts Info
Taxpayer ID
Other: User ID, enrollment accounts, payment information, and Issuer EDGE enrollment and claim data

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The PII purposes:

User identification, validation, and authorization (name, email, and phone number). The information is needed to create user accounts as well as complete any help desk service request that is initiated by the individual.

RADV audit. PII for individuals is collected by the system for individuals enrolled in the medical plans covered by the Marketplace. The information is needed to audit the accuracy of the information on the EDGE servers.

IDR TA RE
Eligibility data for Federal IDR processing: Dispute # + Claim # + Service Code + Date of Service (PHI).

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.

5 U.S.C. § 552a(e)(3)
Sections 9816(c) and 9817(b) of the Internal Revenue Code
Sections 716(c), 717(b) of the Employee Retirement Income Security Act of 1974 (ERISA)
Sections 2799A-1(c), 2799A-2(b), 2799B-4(b)(3), 2799B-1, 2799B-2, 2799B-3, 2799B-5, 2799B-7, 2719, 2723, and 2761 of the Public Health Service (PHS) Act
Section 1321(c) of the Affordable Care Act.
CAA of 2021 became Public Law No: 116-260 on December 27, 2020. Two acts within the law apply to CCIIO: Title I, "No Surprises Act." and Title II, "Transparency

5 USC 301, Departmental Regulations.

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.

09-70-0511 CMS Risk Adjustment Data Validation System (RAD-V)

09-70-0516 Complaints Against Health Insurance Issuers and Health Plans (CAHII)

09-70-0560 Health Insurance Exchanges (HIX) Program

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
State/Local/Tribal
Non-Governmental Sources
Public
Private Sector

Identify the OMB information collection approval number and expiration date

OMB collection approval number 0938-1187 - expiration date 06/30/2025

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.

Data Use Agreements (DUA's):
MATS/SPIDR DUA CONT-2021-56912
Payment Policy and Financial Management Group (PPFMG) Premium Stabilization Programs and Marketplace Operational Support DUA CONT 2014-27183

Describe the procedures for accounting for disclosures.

The CCRMS follows the CMS/ HHS Vulnerability Disclosure Policy, as well as the CMS.gov Privacy Policy.

Disclosure Statement: “HHS is committed to timely correction of vulnerabilities. However, we recognize that public disclosure of a vulnerability in absence of a readily available corrective action likely increases versus decreases risk. Accordingly, we require that you refrain from sharing information about discovered vulnerabilities for 90 calendar days after you have received our acknowledgement of receipt of your report. If you believe others should be informed of the vulnerability prior to our implementation of corrective actions, we require that you coordinate in advance with us.

We may share vulnerability reports with the Cybersecurity and Infrastructure Security Agency (CISA), as well as any affected vendors. We will not share names or contact data of security researchers unless given explicit permission.”

For more details, reference the Vulnerability Disclosure Policy | HHS.gov

Privacy Policy: Protecting your information is very important to us. This privacy policy describes what information we collect, why we collect it, and what we do with it, available at Privacy Policy | CMS.

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

No prior notification is required. PII data that is collected is through the plan sponsors or organizations who participate in the Federally Funded Marketplace.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

There is no "opt out" feature required. The information is required for identification, validation, and authorization by the individual to complete the help desk transaction.

IDR TA RE

Not Applicable. The IDR TA RE accesses existing Independent Dispute Resolution cases and is not operationally collecting information.

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

CCRMS sub systems contain privacy statements on each of the forms completed by the plan sponsor or organization. Normally, no further notifications are required once the user completes the form validation and verification process. A user would be notified via email of major system changes.

IDR TA RE

Not Applicable. The IDR TA RE accesses existing Independent Dispute Resolution cases will not notify patients as part of operational directives.

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 individual may contact the specific work stream Help Desk directly by email. This process initiates a ticket number by which a Help Desk agent will respond appropriately to the contact information the user provided.

IDR TA RE

The collection of dispute resolution data is not the responsibility of the IDR TA RE and will not notify

patients.

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

The CCIIO Customer Relations Management Team conducts reviews of any discrepancies reported by either automated auditing controls, user submitted discrepancies, or manual auditing. Any variation in the accuracy or integrity of the information is logged and reported to CCIIO leadership with details of the audit and additional actions taken for remediation.

IDR TA RE

The IDR TA RE does not store, maintain, or share PII/PHI. The IDR TA RE uses data for eligibility purposes for the Federal IDR process on existing CMS IDR Salesforce data.

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.

The administrative procedures in place to determine which system users may access PII are authentication and authorization rules that give specific permissions to each user role. Role-based access is based on the principle of 'least privilege' where users are given 'need to know' and 'need to access' permissions. All user roles and authorizations for the system are documented in the CCRMS System Security and Privacy Plan (SSPP). Acquiring PII within Salesforce requires individuals to access either CMS IDM or username/password with two factor authentication enabled.

IDR TA RE

Analysts and Developers have access to PII/PHI. Analysts are performing job/role-based tasks related to Independent Dispute Resolution Technical Assistance. Developers are ensuring operational environment security, compliance, and performance.

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 system controls in place for access to PII include role-based access permissions, and limits on the PII that is displayed so that only the minimum amount of PII is visible to users. Users are assigned different roles corresponding to different levels of access to data as well as the ability to perform specific actions (e.g., read, update, delete).

IDR TA RE

The IDR TA RE is Role-Based Access Control (RBAC) compliant and governed by the federated EUA credentialing and authorization process. Only two user roles are present: Analyst and Developer.

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 CCRMS personnel undergo corporate and project-specific training at time of hire and annually

thereafter. This training includes the CMS Information Systems Security and Privacy Awareness (ISSPA) course (mandatory for all users of CMS Information Systems when users are initially issued their CMS User ID) and review/ signature of the HHS Rules of Behavior, with content specific to the protection of PII.

IDR TA RE
All IDR TA RE users must comply and complete CMS User ID Certification, CMS Information Systems Security and Privacy Awareness training, and Cyber Awareness Training to maintain EUA compliance.

CCRMS personnel must also complete project-specific training before starting work on the project or receiving access to additional roles within CCRMS.

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

CCRMS personnel are to complete role-based training on at least an annual basis. Training courses are provided by the agency or contractor and include content about updates to the Cloud Service Providers (Amazon Web Services, Salesforce), policy and procedure updates, and proper use of the information system.

IDR TA Analysts may receive additional training to use/perform analysis tasks on the IDR TA RE user interface (https://ui.impl.idrta.internal.cms.gov).

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.

CCRMS operates in accordance with the CMS CCIIO Records Retention Schedule File Plan, National Records Association (NARA), and General Records Schedule (GRS) 3.2 (N1-GRS-07-3 item 13a2).

IDR TA RE
The IDR TA RE temporarily accesses PII/PHI from CMS IDR Salesforce and persistent S3 buckets within the CCRMS environment. The PII/PHI data that is temporarily accessed to verify dispute resolution accuracy is briefly stored in a PostgreSQL database. The IDR TA RE AI model temporarily accesses PII/PHI for model training; the training period for the AI model is less than 24 hours. When AI model training is complete, the redundant data that is temporarily stored in the PostgreSQL database is then purged. IDR TA RE is not tasked nor required to retain or delete PII/PHI that it temporarily accesses from CMS IDR Salesforce or persistent S3 buckets.

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

PII is secured in the system using administrative, technical, and physical controls, in accordance with policies and regulations detailed in the CMS Information Security Acceptable Risk Safeguards-Minimum Security Requirements (ARS).

Administrative controls include role-based permissions to access CCRMS web pages and applications, request and authentication through the CMS IDM system, security and network policies and procedures as well as security and privacy training regarding securing PII.

Technical controls include role-based access, inactivity timeout, multi-factor authentication, data encrypted at rest, data encrypted while being transmitted electronically, network firewall, anti-virus/malware prevention, intrusion detection/ prevention technologies, centralized event log monitoring and event alerts.

CCRMS, hosted in the cloud inherits physical security controls from the FedRAMP Salesforce Government Cloud and Amazon Web Services GovCloud and Commercial.

IDR TA RE
Given the sensitive nature of the IDR dispute data being processed, security is of paramount importance. The RE architecture employs a combination of AWS security services and best practices to ensure data confidentiality, integrity, and availability. Key security practices utilized in the RE design include:
Intrusion Detection and Prevention (IDP): AWS GuardDuty continuously monitors the AWS environment for unauthorized or malicious activities. Detected anomalies are flagged, and alerts are forwarded to AWS Security Hub for further investigation.
Role-Based Access Control (RBAC): Access to resources is restricted using IAM policies based on the principle of least privilege. This ensures that users and services only have access to the minimum resources necessary to perform their tasks.
Encryption: Data is encrypted both in transit and at rest using AWS-managed keys. Sensitive information stored in S3 is encrypted using Server-Side Encryption (SSE), and future environments will incorporate KMS for additional key management security.

Identify the publicly-available URL:

https://nsa-idr.cms.gov/billdisputes

https://nsa-idr.cms.gov/providerresponse

https://nsa-idr.cms.gov/idreapplication
Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null