# US Department of Health and Human Services

## Privacy Impact Assessment

**Date Signed:**

12/21/2021

**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.**

PIA Validation

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

Title I (No Surprises Act) and Title II (Transparency) of Division BB of the Consolidated Appropriations Act, 2021 (CAA), establish new protections for consumers related to surprise billing and transparency in health care.

The legislation contains new requirements for group health plans, health insurance issuers in the group and individual markets, providers, facilities, and air ambulance providers.
CAA provisions require CCIIO to implement a federal IDR process that must be operational by January 1, 2022. As part of this process, CMS must enable IDR parties to select a mutually agreed-upon, qualified federal IDRE (or have one assigned if they cannot agree), track cooling-off periods, and capture arbitration case data. On a quarterly basis, CMS must report data on the use of the IDR process. Other agencies involved in the IDR provisions include DOL and IRS. CCIIO's responsibilities include the implementation of IDR operations and system solutions for all agencies.

These system modifications aim to provide an independent pathway for issuers, providers, and consumers to settle payment disputes and will provide information on payment practices to inform future policy making.

Successful administration of the IDR system enables the efficient resolution of disputed cases regarding transparency or surprise billing at the federal level and consistent, accurate tracking and reporting of IDR data.
Approach:
The solution will be comprised of three pieces:
Public sites for Claimant and Respondent to initiate their dispute and/or provide supporting documentation.

IDR Portal (Salesforce Community) where the IDR and SDR Entities will log in to review assigned work and document COI's, fee payment, dispute results, etc.
API between CCRMS-MATS IDR module and CCRMS-RARI VM module for passing the User Fee debits and payment reports back and forth.

Since consumers will use a public site instead of logging into the Salesforce Portal, there is a risk that PII and PHI could be compromised when consumers are using shared devices. The new solution will include a script that terminates the session and clears the data if the user allows the application to be inactive for more than 15 minutes, so any IIHI entered is removed from the public facing page and browser.

**Describe the purpose of the system.**

The Center for Consumer Information and Oversight (CCIIO) Customer Relations Management System (CCRMS) is a system is composed of four (4) Salesforce organizations (orgs) that are managed by one contractor whose sole purpose is to provide customer service support related to the Affordable Care Act (ACA). These orgs are:
Re-Insurance Contribution System (RICS) which receives and processes inquiries from plan sponsors.
Risk Adjustment and Re-Insurance (RARI) which is comprised of three programs to include Risk Adjustment Data Validation (RADV), Vendor Management (VM), and External Data Gathering Environment (EDGE) program.

Marketplace Assisters Technical Support (MATS) which is responsible for collecting and processing inquiries from Marketplace Assisters.
System Plan and Issuer Data Reporting (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.

The CCRMS system utilizes EZProtect which is the antivirus solution. EZProtect is a virus scanning application that scans chatter files, documents, attachments, and content for harmful viruses. The EZProtect antivirus solution scans all Salesforce file types including, Attachment, Content Document, Document, and Static Resources. The Consolidated Appropriations Act (CAA) of 2021 became Public Law No: 116-260 on December 27, 2020. Two acts within the law apply to CCIIO: Division BB, Title I, "No Surprises Act." and Title II, "Transparency. “CCIIO assessed the provisions in Titles I & II and determined that it needed to: Develop policy to further define the details of the provision. Implement operational processes and technical functionality to support operations of the provisions. Coordinate across CMS (e.g., with ASPE) and with Department of Labor, Department of Treasury, and Department of Transportation according to the legislation. From those provisions, seven workstreams were identified that required CCIIO to build new or modify existing system functionality. Of these seven, the Independent Dispute Resolution (IDR) and Complaints workstreams were added to Marketplace Assisters Technical Support (MATS). Independent Dispute Resolution:

The IDR 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 cases, and build the capacity to collect user fees from disputing parties for use of IDR pathway. The IDR is comprised of the following:

IDRE Application- landing page and application web form for an entity to apply to become a certified IDRE.
IDRE Registration- if application approved, the applicant would receive an invitation to the IDR Entity Community.
IDRE Community- this is an environment where IDREs can renew, re-certify, and/or withdraw their IDRE certification, update their organization/identifying information.
IDRE Certification Process- is a multi-step process using Salesforce to review, evaluate and retain the application data submitted; the review process will help indicate whether the candidate should be eligible to become a certified IDRE. If the application is reviewed and approved to be eligible for certification, there will be a public forum for a petitioning period.

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). The Complaints system is comprised of:
Establishing and publicizing a system solution capable of efficiently receiving, ticketing, triaging, and tracking cases from consumers related to plan, issuer, and/or provider non-compliance with surprise billing provisions • Providing responses to such complaints within 60 days of receipt • Increasing efficiency of working cases and decrease resolution time of open cases through collaboration functionality. Improve other workstreams: i.e., system data can be analyzed and interpreted to determine helpful language for consumer documentation.

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

CCRMS collects, maintains, and stores information at multiple levels: 1) pertaining to individual and company names, email addresses, phone numbers, mailing addresses, and tax payer identification numbers, date of birth 2) enrollment accounts, payment information, Issuer EDGE enrollment and claim data (this is not maintained at the enrollee level), and 3) HHS RADV Sampling Reports, limited individual enrollee claim and medical record data. The information is not shared with organizations outside of the agency. The system does not collect or store user credentials about system users/administrators.

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

Each of the four Salesforce organizations (orgs) that comprise the CCRMS system has an individual purpose.

Each system provides help desk style support for inquiries related to the Affordable Care Act (ACA) marketplace services that the specific org supports. Each system acts as a database and data repository for information. The MATS, SPIDR, and RARI orgs all provide user access to non-CMS users which are typically employees of issuer organizations and those that support/work with the issuers.

The information provided will be stored permanently, and will not be shared with organizations outside of the agency. As a result, the PII that is collected to retrieve system records includes first name, last name, email address and phone number to adequately identify the user authorized to have access. The users authorized to have access are employees, public citizens, patients and Federal, state and local agencies.

**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

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

**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?**

100,000-999,999

**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 the 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.

**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.**

Authority for maintenance, collection and disclosure of information is given under sections 2719, 2723 and 2761 of the Public Health Service Act and section 1321(c) of the Affordable Care Act. Consolidated Appropriations 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

**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.**

Health Insurance Exchange (HIX) Program SORN 09-70-0560, 10/23/2013

**Identify the sources of PII in the system.**

**Directly from an individual about whom the information pertains**

In-Person

Email

Online

**Government Sources**

Within OpDiv

**Non-Governmental Sources**

Public

Private Sector

**Identify the OMB information collection approval number and expiration date**

OMB collection approval number 0938-1187 - expiration date 06/30/2022

**Is the PII shared with other organizations?**

Yes

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

**Within HHS**

The company or plan information is used to validate CCRMS users to obtain a log in to the system. The enrollee level details are used to validate the necessary HHS RADV audits of Issuers.

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

Not applicable

**Describe the procedures for accounting for disclosures.**

Not applicable

**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, validations, and authorization by the individual to complete the help desk transaction.

**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 one the user completes the form validation and verification process. A user would be notified via email of major system changes.

**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 CCIIO Customer Relations Management System 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 initially.

**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 weekly 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.

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

**Administrators:**

Authorized users such as administrators are provided with a minimum necessary system access for each module for the performance of required tasks. Administrators do not regularly access. There are discretionary security controls and audit controls are in place.

**Developers:**

Developers are provided with a minimum necessary system access. Developers do not regularly access PII but only as necessary to perform tasks. Discretionary security controls and audit controls are in place .

**Contractors:**

Direct contractors are responsible for maintaining and supporting CCRMS and are required to view PII data to support Help Desk Services.

**Others:**

Business Analysts and Testers are provided with a minimum necessary system access. Developers do not regularly access PII but only as necessary to perform tasks. Discretionary security controls and audit controls are in place.

**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 Plan (SSP). Access to PII requires two factor authentication to CCRMS.

**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).

**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 security and privacy awareness training with content specific to the protection of PII. CCRMS personnel must also complete project-specific training before starting work on the project or receiving access to additional roles within CCRMS. In addition, all personnel must sign agreements to acknowledge awareness of their responsibilities to protect this information.

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

CCRMS personnel must complete additional project-specific training before starting work on the project. Training courses provided by the agency or contractor include content about correct use of CCRMS as well as how to conduct case analysis and other project activities performed using the system.

**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).

**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 EIDM system, periodic review of users and deletion of non-active accounts, 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, being hosted in the cloud inherit physical security controls from the Federal Risk and Authorization Management Program (FedRAMP) Salesforce Cloud and Amazon Web Services Cloud.

**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.**

Session Cookies that do not collect PII.

**Does the website have any information or pages directed at children under 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