US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/07/2023

OPDIV:

CMS

Name:

Electronic Retro Processing Transmission

PIA Unique Identifier:

P-8500732-371909

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.

Email Notifications to respective user(s) when an event happens within the Electronic Retroactive Processing Transmission application and other functional enhancements as outlined in the Electronic Retroactive Processing Transmission Application Release 4 Requirements document.

Describe the purpose of the system.

In order to allow timely access to services for enrollees of Medicare Advantage and Prescription Drug Plans, the Centers for Medicare and Medicaid Service has acknowledged that the logistics of completing enrollments, action requests and processing documentation can cause routine delays. To alleviate this waiting process for beneficiaries, services and actions can still be provided and their related information are reviewed separately as part of a retroactive actions. To manage this, the Centers for Medicare and Medicaid Service has empowered a Retroactive Processing Contractor to be responsible for reviewing these actions to ensure they are correct. If found incorrect, they are then rejected and handled accordingly.Plan Users / Sponsors of these programs, who represent all

of the beneficiaries that are enrolled under their specific contracts, are responsible for sending Submission Packages of these actions to the Retroactive Processing Contractor. The Retroactive Processing Contractor, in turn, will send their findings on each Submission Package back to the originating Plan User / Sponsor in the form of a Review Package (also known as Enrollment Data Validation, or Packages). The Electronic Retroactive Processing Transmission application replaced physical mailing of paper versions of these Packages between the Plan Users / Sponsors and the Retroactive Processing Contractor. It also provides automatic audit trails for these package and response transfers.

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

The Electronic Retroactive Processing Transmission application uses the Centers for Medicare and Medicaid Services' Enterprise Identity Management system to register and log users into the application. No data from this process is held within the Electronic Retroactive Processing Transmission application for Plan Users / Sponsors. Email addresses and assigned contract numbers are retrieved from the Enterprise Identity Management system and stored for all Regional Office and Central Office users to allow for action notifications on specific contracts but are not accessible by the users.Once authenticated and authorized, Plan Users / Sponsors can upload the data required for Submission Package through the User Interface for their contracts. Each package can have a number of attachments (word, pdf, excel files, etc.) which will be reviewed. The Retroactive Processing Contractor validates and processes retroactive requests for enrollments, disenrollment, Plan Benefit Package changes, health status category changes, state and county code changes, Medicaid removals, and dual-eligibility status changes for Low Income Subsidy and Medicaid beneficiaries. It does this for all Medicare Advantage Organizations, Part-D Sponsors, Cost-Based Plans, Program for All Inclusive Care for the Elderly Organizations, and Medicare-Medicaid Plans.

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

Electronic Retroactive Processing Transmission is a web-based portal to provide the Plan Users / Sponsors a secure place to upload the Package data in the form of excel, word, graphic and Portable Document Format files. Each package is assigned a unique identifier by the Electronic Retroactive Processing Transmission application, independent of the data entered by the Plan Users / Sponsors. The Packages are composed of Cover Letters, a submission spreadsheet (one tab in a template is used depending on which kind of package it is), and additional documentation attachments.These packages are securely downloaded by the Retroactive Processing Contractor, who review and audit them independently. The Retroactive Processing Contractor uploads to the Electronic Retroactive Processing Transmission application responses in the form of Excel, Word, and the Portable Document Format files for these services as to whether they are proper (for example, Covered under their contract or improper and should be billed instead). These responses are available for the appropriate Plan Users / Sponsors only.The attachments may contain the following information for beneficiaries, which may differ depending on the service in question. The following information is collected for each grouping of actions, as allowed per the Centers for Medicare and Medicaid Services' guidance:Enrollments, Reinstatements, Disenrollment, Plan Benefit Package Changes, and Segment Changes:A Cover Letter from the organization (Word or Portable Document Format files). This contains:Applicable Plan Number(s).Description of what is in the package.Appropriate special circumstances or special handling instructions from an Account Manager.A Retroactive Processing Contractor submission spreadsheet (Specially formatted Excel File) with the following information:Contract NumberPlan Benefit Package (not for State and County Code Changes, Low Income Subsidy, Medicare status changes or removals)Segment (for Plan Benefit Packages, Enrollments, Reinstatements, and Segment changes)Health Insurance Claim Number also known as the beneficiary identifierLast NameFirst NameElection Period (for Disenrollment, Plan Benefit Packages, and Enrollments)Effective DateEnd Date (not for Low Income Subsidy or Disenrollment)Application Receipt Dates (for Plan Benefit Packages and Enrollments) Additional information for Low Income Subsidy only: Beneficiary Date Of Birth, State of Residence,

Dual Eligible Status, Institutional or Home and Community-Based Services Status. Additional Information for State and County Codes Changes only: Requested State and County Codes Changes and Zip Code.Documentation for each beneficiary supporting the retroactive transactions (These can be Office Suite files, Portable Document Formats, or Image Files).Regional Office Approval Letter (if applicable).

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

Yes

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

The PII stored within the RPC Submission spreadsheet attachments for packages from Plan Users /

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

Patients (Beneficiaries enrolled in Medicare Part C and Part D Plan).

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

The Personable Identifiable Information in Submission Packages is used to determine whether the transactions, services or requests were legal and valid through the Retroactive Processing Contractor auditing process.The Enterprise Identity Management Personable Identifiable Information is used to notify individual Regional Office users that are assigned to a specific contract when action is needed.

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.

10332 of the Patient Protection and Affordable Care Act

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

No

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

N/A

Is the PII shared with other organizations?

Yes

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

Private Sector. The Retroactive Processing Contractor is authorized to download packages and the attachments containing Personable Identifiable Information in order to perform the necessary audits required for Retroactive Processing. This auditing process is done offline, with a report of the findings uploaded to the Electronic Retroactive Processing Transmission application independently via a dedicated, secured channel. Additionally, all Plan Users are health care providers who are submitting the information for the specific contracts they have with this agency, and in turn reviewing the responses from the Retroactive Processing Contractor.

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

The Retroactive Processing Contractor has a Memorandum of Understanding as well as an Information Sharing Agreement. The application development contractor has a Data Use Agreement.

Describe the procedures for accounting for disclosures.

Review of the Information Sharing Agreement between the Retroactive Processing Contractor and the Electronic Retroactive Processing Transmission application occur and are tested annually. The Centers for Medicare and Medicaid Services Privacy Office keeps an accurate account of disclosures through the use of the Data Use Agreement. This captures Date, Nature, and Purpose of the disclosure as well as the Name and address of the requesting person/agency. The Centers for Medicare and Medicaid Services currently retains the Data Use Agreement over the life of the record. Plan Users can request disclosures of Personable Identifiable Information from the Centers for Medicare and Medicaid Services. Within the Information Sharing Agreement, parties are required to report privacy breeches or suspected breaches to the Centers for Medicare and Medicaid Service within one (1) hour of detection.Disclosure of privacy information between systems is managed under routine use notices. In addition, audit logs maintain transaction information only (not the Personable Identifiable Information itself) as a record or accounting each time it discloses information as part of a retroactive enrollment procedural review.

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

The Electronic Retroactive Processing Transmission application does not collect Personable Identifiable Information directly from the individuals. This information is supplied by the Plan Users and Sponsors about which they have direct agreements with.All user information from Regional Office users (email addresses) are provided from another Centers for Medicare and Medicaid Service, Enterprise Identity Management. The Enterprise Identity Management Privacy Impact Assessment provides the process by which they notify individuals regarding its 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.

There is no option to opt-out of the collection or use of Personable Identifiable Information because this information is required by Retroactive Processing Contractor to review and process the requested retroactive processing on behalf of those affected.Regional Office's may not opt-out of providing the email address information as they are used to send them notices of packages requiring their prompt attention and action.

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

The Personable Identifiable Information within the Electronic Retroactive Processing Transmission is provided through submittal from Plan Users and Sponsors on behalf of those the Personable Identifiable Information relates to. This is documented within the Data Use Agreement, and not collected directly from the individuals.If a major change, the System of Records Notice will be updated and posted on the Department of Health and Human Services website to inform the public. User information from Regional Office users (email accounts) would be addressed by the Enterprise Identity Management’s Privacy Impact Assessment which addresses their process to notify and obtain consent from individual users.

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.

Any individual who has concerns should contact the Centers for Medicare and Medicaid Service through the Privacy Office, which can be done through visiting https://www.hhs.gov/hipaa/filing-a-complaint/. Information about and the ability to file a complaint are available at this website. In the event that the internet is not accessible and you have questions about this topic, the Centers for Medicare and Medicaid Services can be reached by phone at 1-800-MEDICARE (1-800-633-4227). When calling, ask to speak to a customer support rep about Medicare's Privacy Notice. TTY users may call 1-800-486-2048.Individuals who wish to file a complaint directly without access to the internet may directly call the Privacy Office at 1-800-368-1019. TTY users may call 1-800-537-7697 to file their complaints.

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 Electronic Retroactive Processing Transmission application does not collect Personable Identifiable Information directly, and does not address data integrity within documents / packages. All files uploaded are virus scanned and secured to ensure that changes or unauthorized disclosures are prevented.The Centers for Medicare and Medicaid Services has a National Institute of Technology-compliant continuous monitoring program to ensure system integrity and availability for all data submitted to the Electronic Retroactive Processing Transmission. Yearly testing of the system is required to review and update this process for disaster recovery purposes. Back-ups are in place to ensure information is readily available, even if one or more servers should fail.

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

Users. Users are within three distinctions, and all have access to perform their respective business functions: Plan Users / Sponsors - they create packages by uploading related documents to support their requests and handle response packages as appropriate. Central Office Users and Regional Office Users review, respond to and approve packages based on regions impacted and type of request. They also access reports to oversee the performance of the contracts in a particular region and/or parent organization.

Administrators. The Application Administrators and Infrastructure Hosting and Centralized Connectivity Services contractor will perform application oversight and manage related helpdesk tickets for all users.

Developers. Developers will create, test, and maintain the Electronic Retroactive Processing Transmission application and related coding within a segregated development environment; not within the production environment and without Personable Identifiable Information of any type. The developers are also the system administrators.

Contractors. The Retroactive Processing Contractor is the direct contractor responsible for performing retroactive processing review and validation.

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

All user roles (Central Office, Regional Office & Plan Users) are approved by the Electronic Retroactive Processing Transmission Business Owner through the appropriate procedures within the Enterprise Identity Management. Each user is provided a unique role for access to the Electronic Retroactive Processing Transmission, which does not provide access to any data by itself, and to each parent organization's contract that is appropriate for their business role. Authorization for access to individual contracts are performed by the appropriate authority per contract. Administrators are authorized by the business owners, and identified through the application contract. Their access is limited to support functions in support of the helpdesk process. Those in the developer role are not provided direct access to any production data that may contain Personable Identifiable Information. The Retroactive Processing Contractor is designated by the Business Owner through the appropriate procedures dictated by the Retroactive Processor Contract.

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.

As all Personable Identifiable Information is contained within files uploaded to support a particular package, and each package is designated to specific contracts, all data is isolated by authorized access to specific contracts. Further methods to ensure that role-based access is kept segregated can be found in the Enterprise Identity Management's Privacy Impact Assessment.

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 are required to take the annual Centers for Medicare and Medicaid Services' role-based privacy and security awareness training. Internal and external security and privacy staff attend the Centers for Medicare and Medicaid Services quarterly security awareness training and meetings throughout the year to keep abreast of relevant and timely security issues.

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

Central Office, Regional Office and Plan Users are provided role-specific training from the development team on the appropriate usage of the system. Administrators and Developers receive role-specific yearly training for role-based security, which is organizational.

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.

The Centers for Medicare and Medicaid Services has employed a records retention schedule referred to as a "Bucket Approach", or otherwise known as flexible scheduling. More about this approach, what it means, and how it is applied at Federal Agencies can be found on the National Archive's website at: https://www.archives.gov/records-mgmt/faqs/flexible-scheduling.htmlSince the Plan User Personable Identifiable Information are contained in packages that are used for reviewing the compliance and ensuring the integrity of Medicare programs, they are considered part of Bucket 9: Compliance and Integrity records schedule for the Centers for Medicare and Medicaid Services (DAA-0440-2015-0012). All files within this grouping are considered Temporary; they do not have to be transferred for Permanent storage at the National Archives once the amount of time they must be retained is complete. All files within this category must be destroyed after seven (7) years old or when no longer needed for agency business, whichever is later.Every January, relevant files for the previous calendar year are reviewed for deletion based on the date of their creation. For

example, in January of 2018, all the packages created from January to December of 2010 will be reviewed. Packages that are currently part of a legal discovery or otherwise related to active agency business as determined by the system owners / Central Offices will be removed from consideration and kept. All exceptions will be included in the following year’s review. The rest of these packages are then deleted and removed by the system administrators.For Regional Office email addresses, all accounts that were created seven years prior are considered at the same time as the packages described above. If the accounts have not been active for more than a year from the time, the system administrators delete them; it is assumed they are no longer required for the Electronic Retroactive Processing Transmission use.

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

The Electronic Retroactive Processing Transmission data resides in the Centers for Medicare and Medicaid Services Enterprise Content Management environment which is housed in the Baltimore Data Center behind locked doors and is only accessible by approved personnel. All policies relating to information security are addressed in the Centers for Medicare and Medicaid Services organizational security and privacy policy and procedures, including the Centers for Medicare and Medicaid Service policy for Information Security Program and the Acceptable Risk Safeguards. Technical controls include access controls which are established to limit operations and maintenance user access to the data based on role based design and assigned on a need to know basis. Data is protected by the mainframe security configuration and Resource Access Control Facility controls.Administrative and Technical controls for the Regional Office Personable Identifiable Information are addressed by the Enterprise Identity Management System's Privacy Impact System. The application is regularly assessed using the Centers for Medicare and Medicaid Services Federal Information Security Management Act of 2002 security policies and controls that include administrative, technical, and physical controls. All controls are tested within a 3 year period as part of annual Federal Information Security Management Act of 2002 evaluations.