US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/20/2016

OPDIV:

CMS

Name:

Recovery Audit Contractor Region B

PIA Unique Identifier:

P-8178634-085545

The subject of this PIA is which of the following?

General Support System (GSS)

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.

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.

The Ongoing Responsibility for Medicals (ORM) and Non-Group Health Plan (NGHP) software modules were newly implemented in Recovery Audit Center- Region B (RAC-B). NGHP receives its data from the Medicare Secondary Payer Systems Contractor (MSPSC). NGHP works to recover improper payments on claims associated with accidents that may be covered by other insurance policies (i.e., worker's compensation). NGHP includes the addition of diagnosis codes to the system data.

Describe the purpose of the system.

The Recovery Audit Contractor - Region B (RAC-B) supports the CMS Recovery Audit Program’s mission to identify and correct Medicare overpayment's and underpayments to health care providers and suppliers in selected states. The RAC-B reviews the Medicare claims for the states of Michigan, Ohio, Kentucky, Indiana, Illinois, Minnesota and Wisconsin to identify any inappropriately coded claims, process corrections to those claims according to CMS guidelines and provide reporting to CMS.

Additionally, the RAC-B supports the Medicare Secondary Payer Recovery Audit Contractor (MSPRAC) Program. The business function for this program is to review Medicare beneficiary eligibility leads from the MSPSC, identify any claims paid where Medicare should be secondary but paid as the primary, process collections from the employer/insurer (debtor) for those claims according to CMS guidelines, and provide reporting to CMS.

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

RAC-B uses and shares Medicare claims data to identify improper payments made to providers for services rendered to Medicare beneficiaries and refer potential fraud to CMS.

RAC-B also uses and shares Medicare claims data included in the Medicare Secondary Payer (MSP) program for recovery audit contractors. RAC-B handles claims where Medicare has made a primary payment by mistake and seeks recovery from the provider.

Medicare claims data includes: Name; Date of Birth (DOB); Health Insurance Claim Number (HICN); Mailing Address; Medical Notes; Diagnosis Codes; Dates of Service; Payment and Charge Amounts; Physician and Provider Identifiers (IDs), Tax/Federal IDs. Claims data may be compiled into a letter and shared with GHP, NGHP and employers in the recovery process.

RAC-B user information is collected and stored with data recorded on audit logs and transactions processed. Users are CMS contractors who are not HHS employees and do not have HHS credentials. There are no external users for the systems. User IDs, first/last names, and email addresses are collected and stored.

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

The system shares data with other CMS systems to include, CMS Integrated Data Repository (IDR), Benefits Coordination and Recovery System (BCRS), Data Extract System (DES), and the Healthcare Integrated General Ledger Accounting System (HIGLAS). It does not collect PII from Medicare beneficiaries. Data is sent to the Electronic Correspondence Referral System (ECRS), Momentum, and HIGLAS.

For Medicare beneficiaries, the system is used to predict, identify, manage and analyze medical claims; receive data; execute queries; audit results; create and submit adjustments; and generate letters and reports. The data elements listed in PIA-012 are collected in support of letter generation and claims management.

This data is used to evaluate Medicare claims and determine if Medicare should have been the primary or secondary payer. If Medicare should have been the secondary payer and was the primary payer, the system performs the business functions necessary to recover Medicare's misdirected funds. If a beneficiary has Medicare and other health insurance, Coordination of Benefits (COB) rules determine which entity pays first. If a Group Health Plan (GHP) is the proper primary payer, recovery is sought from the employer and GHP. Recoveries are also sought for mistaken NGHP claims where a liability insurer, no-fault insurer or workers' compensation entity is the identified debtor and has ongoing responsibility for medicals (ORM) for specific care or an injury.

Medicare claims needing to be reprocessed are submitted to organizations that handle Medicare claims. Medicare claims due to primary/secondary payer issues will be sent to other insurers or providers. Claims related to NGHP may be sent to patients and/or other insurance providers and payment entities.

User IDs, first/last names, and email addresses are collected and stored with data recorded on audit logs and transactions processed. All users are internal CMS contractors who are not HHS credentialed.

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

Mailing Address

Medical Notes

Taxpayer ID

Other - HICN, Dates of Service, Diagnosis Codes; Payment and Charge Amounts; Physician and

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

Vendor/Suppliers/Contractors

Patients

Other - Public insurance providers

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

PII is used in the claims record to identify a patient and match claims together. Claims are matched using the HICN.

The primary purpose for using PII is to identify improper payments from the medical records to assist in the recovery of overpayments and underpayments.

User credentials are used to access RAC-B to perform the function of the system.

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

RAC B does not use PII for secondary reasons.

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

Authority for maintenance, collection, and disclosures of information is given under: Sections 2719, 2723, and 2761 of the Public Health Service Act, Section 1321(c) of the Affordable Care Act 5 USC Section 301, Title XVIII of the Social Security Act, Section 302 of the Tax Relief and Health Care Act of 2006, and 42 U.S.C. 1395ddd.

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.

(3) 09-70-0558 National Claims History; and (4) 09- 70-0571 Medicare Integrated Data Repository.

(2) 09-70-0536 Medicare Beneficiary Database;

The SORNs used to cover the system are: (1) 09-70-0526 Common Working File [CWF];

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Within OpDiv

Other HHS OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

N/A - direct collection is only for user IDs to enter the system and process data

Is the PII shared with other organizations?

Yes

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

Private Sector

Other insurers that handle Medicare claims and providers with claim information; employers with Medicare beneficiaries on their payroll.

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

Data sharing and operating requirements between RAC-B and the Medicare Administrative Contractors (MACs), the Zone Program Integrity Contractor (ZPIC) and the Qualified Independent Contractor (QIC) are administered through Joint Operating Agreements (JOAs). JOAs are maintained with the following MACs: J5, J6, J8, J9, JJ, J11, J15, JA Durable Medical Equipment (DME), JB DME, JC DME, JD, JE, JF, JH, JK, JL, Railroad Specialty Medicare Administrative Contractor (SMAC), Medicare Secondary Payer Integration Contractor (MSPIC), Benefits Coordination and Recovery Center (BCRC), MSPSC, QIC East, QIC West, and the Administrative QIC (AdQIC).

Data Use Agreements (DUAs) are in place between RAC-B and CMS systems to include CMS IDR, BCRS, DES, HIGLAS, ECRS, and Momentum.

Describe the procedures for accounting for disclosures.

The procedures for accounting for disclosures are documented and managed by the other CMS systems that provide the PII information to RAC-B. Beneficiary name and the last four of the HICN are shared in letters to other insurers and employers, as needed. JOAs are in place as well as DUAs which track the PII that is disclosed, to whom, for what purpose and on what date.

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 process to notify individuals that their personal information will be collected is the responsibility of the CMS systems that provide data to RAC-B.

The System Use Notification notifies the users and system administrators that their personal information will be collected. The user has to accept the terms and condition specified in the System Use Notification in order to log into the system.

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.

Users and system administrators cannot opt-out from providing their User ID. The system does not allow anonymous users. Before a new user accesses the system, training is completed and the user learns what data is stored in the system based on their system usage.

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

The PII RAC-B uses are limited to what is required to perform contractual obligations. Release notes are distributed to the entire RAC-B team before the release is operational in production. There are no business reasons to increase what user PII is collected.

RAC-B does not notify and obtain consent from medicare beneficiaries whose PII is needed to recover improper payments. RAC-B does not interact directly with the beneficiaries. Consent from beneficiaries, if required, would have been received by the source CMS systems that provide claims data to RAC-B (CWF, MBD, NCH, MIDR which all have their own PIAs). All RAC-B system users are Canadian Global Information (CGI Federal) employees. All employees are required to sign an annual certification defining the acceptable use policy. This policy states that all internal users of CGI Federal resources do not have a reasonable expectation of operational and security requirements. When major system changes are planned, system users are notified of the scope of the changes as well as the timeline for implementation. Transition plans are developed with system user input and final transitions are coordinated with advanced notice for system users. System administrators are notified of all major changes that may impact their PII stored in RAC-B. If a major change were to occur, the RAC-B system administrators would be informed using the same language and methodology that was used to notify each system of record of the change.

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.

RAC-B does not collect PII from and interact directly with Medicare beneficiaries. The systems that provide data to RAC-B would be contacted by the concerned beneficiaries.

If a RAC-B user, including system administrators, believes their credentials have been inappropriately obtained, used, or disclosed, they are to report a potential PII incident to the RAC-B Product Support Helpdesk. The instructions to report a potential incident, including required incident details and points of contact, are documented in the CGI Federal Healthcare Compliance Incident Response Procedures. This document also includes the process for the Incident Response Team to review potential incidents and report findings as required. The help desk contacts the RAC-B System Security Officer (SSO) directly if any user has concerns about their PII. The SSO would work with the help desk and follow the CMS source system (CWF, MBD, NCH, MIDR, which all have their own PIAs) project policies and procedures to address and resolve user concerns as applicable.

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

RAC-B has automated audit logging to ensure the data's integrity, availability, accuracy and relevancy. All system activities are captured in logs and reviewed by the assigned monitoring teams to ensure data integrity. Data availability is managed by service level agreements (SLAs). Data accuracy is managed using application edits when the data is entered, by reviewing processing results and system alerts received when audit logging fails. Data relevancy is included in the life cycle activities including requirements and data validation.

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

Users:

Users have access to PII in order to perform the recovery activities for improper payments.

Administrators:

Administrators' access to PII is limited to activities necessary to ensure system activities are logged properly and the data is stored and is available as required

Developers:

Under normal operations, developers do not have access to PII.

If needed to troubleshoot production issues, developers access data using an account that limits their access only to the production environment.

Contractors:

As CMS contractors, CGI Federal users, administrators and developers use RAC-B to provide the recovery activities for improper payments. This includes recovering improper payments and supporting the confidentiality, integrity and availability requirements with the RAC-B system and data

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

RAC-B user access is limited by role assignments. Roles are defined per least functionality requirements - access is limited to the business functions required to fulfill that role. Data permissions support least privilege and business need-to-know principles - within each role, a user's data permissions are limited to the information needed to execute and validate the business functions of that role. All RAC-B users have access to PII. Separation of duties is in place such that system administrators responsible for establishing and maintaining user accounts do not process claims data.

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.

Role based access control coupled with data permissions limit a user's access to the minimum amount of information necessary to perform their job. When a team member's role changes and that change requires different activities and modified data permissions, the user's account is reviewed, activity and data access no longer needed are removed from the user's profile before the new access is added.

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.

Every year all RAC-B employees are required to complete general and corporate security and privacy awareness training as well as review and acknowledge rules of behavior. Posters and flyers are used to remind and educate users. Incident identification and reporting training is also provided. Operational and support personnel are trained in all aspects of their contingency roles and responsibilities. Personnel are trained when they start the role, when system changes occur and at least once a year.

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

RAC-B users are required to complete CMS role-based security and privacy awareness. The RAC-B training policy specifies the annual requirements: what training is required and how many hours of training are required. More specific role-based training is documented in the RAC-B training plan. Training topics are varied and include protecting against malicious software, insider threat, HIPAA Privacy Rule and Security Rule, endpoint protection and cloud security. Just in time refresher training is provided when the need arises.

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.

As defined in the CMS Records Schedule and approved by the National Archives and Records Administration (NARA), data retention and destruction of PII stored in RAC-B follow this guidance:

Medicare Secondary Payer Files (Disposition Authority: N1-440-01-05, Item 1) - Case files are not destroyed. Official recordkeeping copy and related data may be scanned and are placed in an inactive file after final action on the case at the close of the calendar year in which final action was taken.

Destroy 10 years after final action. Source documents are destroyed once the originals are scanned and verified and the quality assurance process is completed.

Recovery Audit Contractor Files - Inputs - destroy/delete source data when data have been entered into the Master File or database and verified, or when no longer needed to support construction of, or serve as backup to, the master file or database, whichever is later. (Disposition Authority: GRS 20, Item 2b) Master Files- cut off at the end of the calendar year an improper payment recoupment or final appeals results.

Destroy 10 years after cutoff. (Disposition Authority: DAA-0440-2012-0007) Outputs - destroy/delete reports when no longer needed for administrative, legal, audit or other operational purposes. (Disposition Authority: GRS 20, Item 4) Documentation - destroy/delete when system is no longer operational (Disposition Authority: GRS 20, Item 11a1)3.

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

The following administrative and technical controls are implemented to secure the PII managed by RAC-B:

User ID and two factor authentication controlled access; firewall; front-end security; network technology.

Access to production data is controlled by role based access control and user account reviews.

Physical controls include secured, controlled and limited access in the RAC-B offices and Expedient Data Centers.