US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/26/2016

OPDIV:

CMS

Name:

Recovery Audit Contractor Regions 1 and 5

PIA Unique Identifier:
P-4602902-085545

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.
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.
No changes have been made since the last PIA.

Describe the purpose of the system.
This information system is used by the CMS Recovery Audit Contractor (RAC) for Region A and is referred to as RAC-A. Region A encompasses the Northeastern part of the United States: Connecticut, Delaware, District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island and Vermont. The purpose of the RAC-A system is for auditing Medicare claims to ensure providers/hospitals are following proper billing guidelines and whether there were any incorrect payments.

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

The RAC-A system maintains patient and provider information in relation to Medicare payment claims. This information is not collected directly by the RAC-A system. The information is collected by CMS' National Claims History (NCH) system which has it's own PIA. The information is transferred once a month to Region A Recovery Audit Contractor (RAC-A) via a secured data file transfer directly from NCH.

RAC-A contains the following information about patients: name, date of birth, mailing address, telephone number, health insurance claim number (HICN), gender, ethnicity, medical notes, medical record information (procedure codes, diagnosis codes, dates of service, total charges, Medicare payment amount).

The system also contains information about providers, such as: National Provider Identifier (NPI), facility name and address, and provider name and telephone number.

RAC-A system users (direct contractors) input a user name and password to access the information in the system.

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

The RAC-A system supports the auditing of paid Medicare claims to determine if the claim was billed accurately and followed standard medical guidelines. The RAC-A system maintains patient and provider information in relation to Medicare payment claims, which is used for verification purposes to ensure the correct records are being reviewed for the audit.

This information may contain the following information about patients: name, date of birth, mailing address, telephone number, health insurance claim number (HICN), gender, ethnicity, medical notes, medical record information (procedure codes, diagnosis codes, dates of service, total charges, Medicare payment amount). The system also contains information about providers, such as: National Provider Identifier (NPI), facility name and address, and provider name and telephone number. There are also copies of correspondence with the providers regarding the accuracy or inaccuracy of a paid claim are stored in the system for record retrieval purposes.

The information is transferred to the system by a secure network connection to CMS. The RAC-A system does not directly connect to any other CMS information system or directly collect this information. The information is collected by CMS' National Claims History (NCH) system which has it's own PIA. The information is transferred once a month to Region A Recovery Audit Contractor (RAC-A) via a secured data file transfer directly from NCH. At the front end of the connection is the CMS National Claims History system. At the back end of the connection is the Recovery Auditors claims auditing system.

RAC-A system users are not CMS employees but direct contractors who are performing services on behalf of CMS or providers that have Medicare claims under audit. All system users input user credentials, a user name and password, to access the information in the system. The user credentials are retained in the system for as long as necessary for access.

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

Phone Numbers

Medical Records Number

Medical Notes

Health insurance claim number (HICN), medical record information (date of service, diagnosis code,

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

Employees

Public Citizens

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The PII maintained in this system is used in identifying and auditing paid Medicare claims. User credentials are used to access RAC-A to perform the function of the system.

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

None

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

Sections 1816, and 1874, 1874(a) and 1875 of Title XVIII of the Social Security Act (42 United States Code (U.S.C.) 1395h, 1395kk, and 1395ll

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.

N/A

N/A

National Claims History (NCH), 09-70-0558 published 9/6/2002 and updated 11/20/2006.

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Identify the OMB information collection approval number and expiration date

Not applicable. There is no OMB approval number because the system does not collect information from 10 or more members of the public, per the Paperwork Reduction Act.

Is the PII shared with other organizations?

No

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

There is no process to notify the Medicare patients whose information is transferred to the RAC-A system because it is not directly collected from them. The system users are presented with a "Security Notice" that advises that PII is being collected and that the user has no expectation of privacy because they are accessing a Federal government computer system. The user must click the "I agree" button to move forward.

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 process to notify the Medicare patients whose information is transferred to the RAC-A system because it is not directly collected from them. The system users are cannot opt-out of providing PII (user name and password) if they wish to access the system and use it.

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

There is no process to notify the Medicare patients whose PII is transferred to the RAC-A system because it is not directly collected from them. The system users would be notified at the initial login page of the RAC-A system.The users would likely need to click a 'consent' or "I agree" button, if there were any major changes to the system.

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-A system users are instructed to contact the RAC-A customer service department by telephone, mailing address or the customer service email address.

Customer Service acknowledges the inquiry within 24 hours then thoroughly investigates the concern and responds to the complainant either via a documented telephone call or written response.

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 RAC-A system is designed with logic checks to ensure data accuracy and integrity. Yearly, the CMS Office of Financial Management (OFM) is required to review and update data collection processes to ensure data collected is relevant and accurate.

In addition, protection of the integrity and availability of PII is reviewed at least every quarter by a series of automated and manual review processes. Databases are updated and validated and are redundant allowing for the availability of the information. The security controls for the database is constantly reviewed to ensure safeguards are in place to protect the data.

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

Users:

The RAC-A users have access to PII to access medical records, scan in documents and medical records, conduct audits, respond to inquiries, respond to appeals, and gather required documents for The Medicare claim audit process.

Administrators:

Administrators have access to the system to support the production environment as part of their roles and responsibilities.

Developers:

Developers have periodic access to the information systems that hold and process PII as part of their job roles and responsibilities. These activities may include post go-live support, bug fixes, or troubleshooting activities.

Contractors:

The RAC-A staff are direct contractors of CMS and in the roles of user, administrator or developer, they will have access to PII in accordance to the various role's job function.

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

RAC-A uses role-based access controls to ensure that users, administrators, and developers are granted access on a "need-to-know" and "need-to-access" for their assigned job duties.

Individuals requesting access must complete an Account Request form prior to account creation and indicates the person's name, email, phone number and access level needed. This form is reviewed and approved by the RAC-A system manager prior to account creation.

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.

There are several methods for restricting access. First, is to program user interfaces to limit the display of PII to only those elements needed to perform specific tasks. Second, is to limit the transmission of PII to validate information rather than copy or pull information form another authoritative source. Third, system administrators review user accounts at least semi-annually. Any anomalies are addressed and resolved by contacting the user and modifying their user data, or by removing their access if no longer required. Activities of all users including system administrators are logged and reviewed by a designated individual to identify any unusual activity.

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.

CMS direct contractor staff who access or operate a CMS system are required to complete the annual CMS Security Awareness training provided annually as Computer Based Training (CBT) course. Contractor also completes our annual corporate security awareness training. Furthermore, the contractor must complete an annual HIPAA training.

Individuals with privileged access must also complete role-based security training commensurate with the position they are working in on an annual basis.

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.

RAC-A follows the CMS Records Schedule, Section III. Medicare - Program Related which cites the National Archives and Records Administration (NARA) Disposition Authority: N1-440-04-3, which states that records will be destroyed after a total retention of 6 years and three months.

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

The RAC-A system is in data center within a surrounding secure area. The security measures in place are the use of dual factor authentication with card key access system and biometrics; an active intrusion alarm system, and video surveillance to monitor and record physical access.

Administrative controls such as written policy, procedures and guidelines have been established for system access. Access to the system is limited to authorized users. Each user is granted access based on the principle of least privilege.

From a technical perspective, PII is secured via firewalls, encrypted transmissions and connections, intrusion detection systems, anti-virus and email content filtering software. Additionally, the use of portable storage devices is blocked.