US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/21/2016

OPDIV:

CMS

Name:

PRI Review System

PIA Unique Identifier:

P-7289605-847397

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.

Since the last Privacy Impact Assessment (PIA), the PRI Review System (the System) was relocated to another data center.

Describe the purpose of the system.

The PRI Review System (PRI) supports Centers for Medicare and Medicaid Services (CMS) activities where medical records, claims data, or a subset of claims must be analyzed or evaluated to identify specific outcomes. Information is securely imported into the system from other CMS systems where the Personally Identifiable Information (PII) are first collected. Reviewers and analysts use secure connections to access the information, where they evaluate it based on specified criteria.

Reports or responses are generated to provide the outcomes of the analysis. This information is then made available to CMS in an appropriate, secure manner. Some examples include the Recovery Audit Contractor (RAC) Validation Contractor, in which sampling of claims processed by the RACs

are analyzed to ensure claims are not being inappropriately denied. Another example is the Workers Compensation Medicare Set-Aside Arrangement, where analysts review workers compensation claims involving Medicare to determine appropriate set-aside funding for future payments.

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

The PRI Review System maintains some or all of the following information as needed for a review or study: Medicare claims information, Medical records associated with claims under review or study, Beneficiary information, Provider information, and Device identifiers associated with Durable Medical Equipment (DME). In addition, the following information are maintained in the system:

Coverage Gap Discount Reconciliation (CGDP):

Name, Email, Telephone, Appeal Date, Drug Reaction Network (DRN) Drug Number, Invoice ID, Manufacturer Name, Location
Electronic Health Records (EHR): Provider Organizational Name, Provider Address (Street, Suite, City, ZIP), EHR Denial
Code, Submitter Name, Submitter Address, Sender email address, National Provider Identifier (NPI) Number, Hospital Name, Hospital Address (Street, City, ZIP), CMS Certification Number (CCN), Reviewer/Analyst name, Hardship Case Number, EHR Product Name, Hospital CMS EHR Certification ID, Physician Group Practice, Practice Address

Recovery Audit Contractors Validation Contractor (RACVC):

International Statistical Classification of Diseases and Related Health Problems (ICD) revision 10 (ICD-10) Codes, Medical Record Number, Health insurance claim number (HICN), Provider Name, Provider State, Recovery Audit Contractor (RAC) Region, Beneficiary Name, Claim Amount, Beneficiary Date of Birth (DOB), Beneficiary Address, Admission Date, Discharge Date, Discharge Status, Prescription (RX) Amount Paid, Provider ID, Provider Name, Provider Address, NPI, Provider Type, Healthcare Common Procedure Coding System (HCPCS) codes, Current Procedural Terminology (CPT) codes, Drug Name

Workers' Compensation Review Contractor (WCRC):

Drug Name, Drug Dosage, Drug National Drug Code (NDC), Workmen’s Compensation Date, Prescription ID, Prescription Type, Drug Cost, Total Property Settlement, Total Property Set- aside, Medical Set-aside, Prescription Set- aside, Annuity amount, Gender, HICN, Beneficiary Age/DOB, Beneficiary Date of Death, Beneficiary Name, Beneficiary Address, Beneficiary Telephone Number, Date of injury, Rated/Projected Age, Medical Case Condition Category/Description, Submitter Name, Insurer Name, Insurer Address, Case Designee Name, Procedure codes, Diagnostic Codes, Employment start/end date, Medical Record Information, Social Security Number (SSN) associated with case, Employer ID, Employer Address, Life Expectancy, Injury date.

Credentials

Only personnel accessing the data within the PRI Review System are PRI (direct contractor) employees and CMS employees in the office of primary interest. All access is granted per provisions of the CMS access security controls policies and procedures. The access request is approved by the business/operations management, than provisioned by account administrators. Access is requested and approved based on roles-based separation of duties, with least privilege and need-to-now precepts being applied to minimize and accurately assign rights and privileges.

Each approved user accesses the application via an encrypted secure authentication protocol using their assigned user ID and password. A successful authentication would involve the correct

presentation of a username and password, and a Personal identification Number (PIN) which must be verified by the secured authentication protocol.

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

The PRI Review System uses that data obtained from other CMS systems to analyze and report on the Medical Care program. For each of the four facets of the PRI Review System, this review is specifically focused on mandated facets of Medicare and
Medicaid services.

CGDP

The PRI Review system assists CMS in analyzing Prescription Drug Event (PDE) data to understand how many discounts have been provided in the coverage gap and for which classes of prescription drugs.

EHR Determination

Congress, under the American Recovery and Reinvestment Act of 2009 (ARRA), mandated that payment adjustments should be applied to Medicare eligible professionals, eligible hospitals, and Critical Access Hospitals (CAH) that are not meaningful users of Certified Electronic Health Record (EHR) Technology under the Medicare EHR Incentive Program. The EHR Determination part of the PRI Review System reviews reconsideration requests for hardship exceptions from eligible professionals (EPs), eligible hospitals, and CAHs.

RACVC

The Recovery Audit Contractor (RAC) Validation Contractor (VC) reviews RAC claim determinations on Medicare claims that were paid under Part A or B of title XVIII of the Social Security Act, and to ensure that the RACs are not unnecessarily denying Medicare claims that were properly paid.

WCRC

The WCRC review, IAW CMS guidelines, and acting as an impartial entity, evaluates Workers Compensation Medical Set-Aside (WCMSA) proposals and independently project the future medical costs, including prescription drugs and durable medical equipment, related to the Workers' Compensation injury, illness, or disease, that would be otherwise reimbursable by Medicare.

Overall Summary

The System contains the information needed to perform the appropriate analyses of provided and projected medical treatment. This information varies from project to project, and contains claims information, associated medical record information, associated beneficiary information, provider information, reviewer notes, review and appeals findings, and review and appeals reports. Review and appeals findings reports are shared with CMS. Information is maintained within the system as required by the particular review or study.

CMS employees and PRI direct contractors are users of the PRI Review System. They use their user ID, passwords and PIN to gain system access.

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

Device Identifiers

Employment Status

Other - NPI, CCN, EHR Denial code, EHR certification code, Hardship Case Number, EHR Product

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

Patients

Providers

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

Personally Identifiable Information (PII) is used exclusively to perform the review or analysis of claims. User ID, password and PIN, as credentials for accessing the application, are held for each authorized user and used in order to gain system access for system support.

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

Not applicable.

Describe the function of the SSN.

The Social Security Number is used to identify the beneficiary.

Cite the legal authority to use the SSN.

The Medicare Secondary Payer Mandatory Reporting Provisions in Section 111 of the Medicare, Medicaid, and SCHIP Extension Act of 2007 (See 42 U.S.C. 1395y(b)(7)&(b)(8))

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

Section 1893(h) of the Social Security Act Section 302 of the Tax Relief and Health Care Act of 2006 Sec. 1862. [42 U.S.C. 1395y] (b)(8)(G)
42 CFR 495.102.a(3)
Section 402(a)(1)(J) of the Social Security Amendments of 1967 (42 U.S.C. 1395b- 1(a)(1)(J)).

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.

09-70-0591 Master Demonstration, Evaluation and Research Studies for Office of Research,

09-70-0537 – Workers Comp Set Aside File (WCSAF)

09-70-0558 – National Claims History (NCH)

Identify the sources of PII in the system.

Other

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

N/A

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.

No prior notice is given as this information is provided by another CMS system. For personnel that are authorized to have access to the system, a System Access Form is completed by the user, with the rationale and the type of access to be requested.

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.

Individuals cannot opt out of the collection of their information because information is not collected directly from individuals for this System. Information is obtained from another CMS system, which handles all communications with individuals, including whether they want to opt out or not. If an individual chooses to opt out they will communicate the fact directly with CMS. CMS will then inform the operators of this System. If the information has already been provided for use by this System, it will be removed and notification provided to CMS.

For personnel that have authorized access, a System Access Form is completed by the user, with the rationale and access to be requested. This is voluntary. However, refusal to submit information for a user ID will preclude a requester from getting access to the system.

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

Since this system does not collect the PII directly from individuals, the disclosure and/or data use will be made at the direction of CMS in the event of any major changes to the system. The applicable System of Record Number (SORNs) that supply data to PRI is published for public comment when a change has been made to the collection or disclosure of the data.

All major system changes concerning personally-identifiable information (PII) are published for comment in the Federal Register as part of a modification of the applicable System of Record (SOR).

09-70-0558 – National Claims History(NCH) 09-70-0537 – Workers Comp Set Aside File(WCSAF) 09-70-0591 Master Demonstration, Evaluation and Research Studies for Office of Research, Development and Information (ORDI) (DERS)

Employees who provide their PII in order to obtain access to the PRI System are notified via email if any changes would be made to the system affecting how their PII will be used, collected or

disclosed.

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.

An individual record subject who wishes to know if this system contains records about him or her should write to the system manager who will require the system name, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), and social security number (SSN) (furnishing the
SSN is voluntary, but it may make searching for a record easier and prevent delay)

An individual seeking access to records about him or her in this system should write to the system manager and reasonably specify the record contents being sought. (These procedures are in accordance with Department regulation 45 CFR 5b.5 (a)(2)).

To contest a record, the subject individual should contact the system manager, and reasonably identify the record and specify the information being contested. The individual should state the corrective action sought and the reasons for the correction with supporting justification. (These procedures are in accordance with Department regulation 45 CFR 5b.7.)

System Manager:
Director, Center for Program Integrity, The Centers for Medicare & Medicaid Services, Division of Recovery Audit Operations.

For access to the system, authorized access is requested on a System Access Form is completed by the user, with the rationale and access to be requested. As this information is subsequently available to the user upon provision of credentials to access the system, a new System Access Form can be submitted if there are errors or inaccuracies.

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

Information is received from other CMS systems for use in this System on a quarterly basis. All data is checked upon import to ensure that the received information is syntactically complete and semantically relevant. Once the data is in the environment, information stores are backed up in accordance with CMS requirements, and backup tapes checked for integrity and proper operation. Database integrity checks are conducted on a scheduled basis to insure that information has not been changed. Functionally, reviewers assess the completeness, relevancy, and accuracy of claims and associated documentation as part of the review process integral to the work process. User access is reviewed on a periodic basis to ensure that only authorized personnel continue to have access to the system.

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

Users:

Users require access to review claims which is integral to the work to be performed. These users are vetted, trained and authorized employees of the organization.

Administrators:

System administrators do not always have access to PII. They only have access to PII when they are working within the production system for operational maintenance or for troubleshooting. This is performed as part of their production support functions.

Developers:

Developers are occasionally required to provide production support for break fix or defects in production. PII is never transferred to a nonproduction environment for development purposes.

Contractors:

The PRI Review System is a direct contractor- managed system. Direct contractors need access

to the personally-identifiable information (PII) to support system operations and maintenance.

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

Access to information is based on a user's specific job function, or role. Each role is evaluated for the minimum necessary access levels needed for the role to perform the task(s) associated with the job. These roles are formally validated, and serve as the basis for all access to PII. When an individual is hired, they are assigned the role required to perform their duties. Access request must be approved by the individual's manager before they can be assigned to that role.

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 two elements to ensure that employees only have the minimum access to PII within the system. First, job functions or roles within the system are evaluated to determine the permission level required for both the job function and the information needed to perform that function. These permissions are carefully assessed to ensure that the permission allows only the minimum access required to perform the job, and nothing more. This evaluation is a formal process, and is presented to senior leadership for acceptance prior to moving forward. Second, the permissions are implemented in the system. This is done by assigning the permissions to a system group, or role. For example, permissions needed to perform maintenance on the system are assigned to an Administrator group. Once these groups are constructed, individuals who are qualified, have been pre- screened, and understand their jobs are assigned to a group within the system. Once within the group the individual can only perform the functions for which they have been cleared.

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 those associated with system functions are required to gain a thorough understanding of their security and privacy responsibilities prior to accessing the system. This understanding is accomplished through a battery of training events, including Information Technology (IT) Security and Awareness Training, Rules of Behavior Training, Conflict of Interest Training and Disclosure, Portable Device and Removable Storage Training, Social Networking Training, Phishing Awareness Training, and Health Information Portability and Accessibility Act (HIPAA) Privacy Training. Users are required to attest to the completion of this training prior to accessing the system. Refresher training is provided within 365 days every year thereafter.

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

All system users receive in depth orientation and training by managers to ensure that they understand the proper operation of the piece of the system which is relevant to them. This training includes not only proper function, but proper care for CMS Sensitive and Corporate sensitive information. They receive and are required to annotate understanding of training spelled out in the organization employee manual.

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.

Each time a project is undertaken within the System, specific timeliness and guidance is provided for the duration of retention of PII. While being retained, PII is held in a pre- designated, authorized environment. All PII is encrypted, and access only authorized to those who specifically need it for their job function.

When it is time to be destroyed, PII is destroyed based on the media on which it is stored. If stored on system storage, it is carefully inventoried prior to destruction. Once the inventoried PII is validated as the correct information, it is deleted using federally approved data deletion methods so that it cannot be restored. Once this destruction is complete the information is checked to ensure that it is no longer available for use, and this
fact is kept on file. If information is on physical media such as compact disk (CD) or Digital Video Disk (DVD), the same pre-destruction procedures are followed. Actual destruction is performed by physical destruction of the media with media pieces shredded afterward.

All records in the system are retained in accordance with the National Archives and Records Administration (NARA) General Records Schedule (GRS) 3.2 or when no longer needed for business, whichever is later.

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

PII is secured using administrative, technical, and physical controls. Administrative controls include extensive screening and background checks for all employees, security and operational training prior to system access and annually thereafter, policies and procedures to provide guidance and articulate expectations, assurance of minimum necessary access to information based on role, and comprehensive management oversight. Technical controls include encryption of all PII while it is being stored and while it is being transmitted both internally within the System and to external entities when appropriate. All equipment associated with the System is configured to federal configuration standards. Networks are configured to detect and prevent unauthorized access from outside the System environment as well as from within. Antivirus software ensures that no corrupted or virus-infected files are allowed to be within the system. Physical controls include controlled access to the System data center. The facility and data center are badge access controlled and monitored through a surveillance camera system. Environmental controls, fire suppression, and backup power are available to help maintain a proper operating environment. Contingency plans are in place to minimize the impact should a disaster occur.

Session Cookies that collect PII.

Persistent Cookies that collect PII.