US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:
04/04/2016

OPDIV:
CMS

Name:
Benefits Coordination and Recovery Center

PIA Unique Identifier:
P-8296050-314879

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?
New

Does the system have Security Authorization (SA)?
Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.
The Benefits Coordination and Recovery Center (BCRC) is responsible for customer service and business processes to assist in the proper payment of medical insurance benefits to or on behalf of entitled beneficiaries to support the Coordination of Benefits and Recovery (COB&R) mission. The system prints and mails correspondence and questionnaires. The BCRC's Interactive Voice Response (IVR) does automated handling of phone calls from Medicare beneficiaries, attorneys, providers, employers, and insurers. The BCRC system also provides a graphical user interface (GUI) for the call center representatives to the various COB&R Medicare Secondary Payer System Contractor (MSPSC) systems.

The COB&R program is responsible for all activities that support the collection, management, and reporting of other insurance coverage of Medicare beneficiaries, and the collection of conditional payments or mistaken primary payments that should have been paid under a Group Health Plan (GHP) or as part of a Non Group Health Plan (NGHP) claim.

Describe the type of information the system will collect, maintain (store), or share.
The Benefits Coordination and Recovery Center (BCRC) collects information regarding Medicare Secondary Payer(MSP) information. Data collected includes Medicare beneficiary social security number (SSN), health insurance claim number (HICN), name, date of birth, phone number, medication notes, taxpayer ID, mailing address, insured individual's insurance provider ID, and employment status. The data obtained by imaging the incoming correspondence is stored temporarily in the BCRC system for quality assurance (to ensure the scan is accurate) and to ensure processing completion (the image file is uploaded into another CMS contractor's system for permanent storage). The data obtained during phone calls is used by the BCRC staff to input data into another CMS contractor's system. The phone call itself is recorded and stored temporarily for quality assurance purposes. The data is permanently stored in systems maintained by other CMS contractors (Medicare Secondary Payer Systems Contractor (MSPSC)). The BCRC system users, CMS employees and CMS contractors, use a user ID and password to access the system.

Provide an overview of the system and describe the information it will collect, maintain (store), or share.
The Benefits Coordination and Recovery Center's (BCRC) systems are primarily used to handle telephone inquiries, structured and unstructured correspondence received in the mail room and determine and collect on Medicare Secondary Payer (MSP) accounts receivables. In order to identify callers, Social Security Number (SSN) or Health Insurance Claim Number (HICN), name, date of birth, and phone number are collected. To update MSP records as appropriate, medical notes, taxpayer ID, mailing address, insured individual's insurance provider ID, and employment status are collected. The BCRC system users, CMS employees and CMS contractors, use a user ID and password to gain system access in order to update the MSP records.

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
Mailing Address
Phone Numbers
Medical Notes
Employment Status
Taxpayer ID
Other: Insured individual's insurance provider ID, employment status, medication notes, HICN, user ID

Indicate the categories of individuals about whom PII is collected, maintained or shared.
Employees
Public Citizens
Vendor/Suppliers/Contractors
Other: Beneficiaries

How many individuals' PII is in the system?
1,000,000 or more

For what primary purpose is the PII used?
The Personally Identifiable Information (PII) is used to identify callers (Medicare beneficiaries, attorneys, provider, employers, and insurers) as well as to validate primacy of payment (e.g., insurance coverage other than Medicare). User ID and password are used for the BCRC system access.

Describe the secondary uses for which the PII will be used.
None

Describe the function of the SSN.
Social Security Numbers (SSNs) are used for beneficiary identification purposes only.

Cite the legal authority to use the SSN.
42 U.S.C. 1395y(b)(7)&(b)(8)

Identify legal authorities governing information use and disclosure specific to the system and program.
42 U.S.C. 1395y(b)(7)&(b)(8); sections 1816, and 1874 of Title XVIII of the Social Security Act (42 United States Code (U.S.C.) 1395h, and 1395kk).

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.
09-70-0571, Medicare Integrated Data Repository (IDR)
09-70-0526, Common Working File (CWF)
09-70-0502, Enrollment Database (EDB)
SORN is In Progress

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Hardcopy
Other

Non-Governmental Sources
Public
Private Sector
Other

Identify the OMB information collection approval number and expiration date
OMB# 0938-0565, Exp. 04/30/2017

Is the PII shared with other organizations?
Yes

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

Private Sector
The beneficiary's attorneys, representative, the employer and insurer to establish primacy of payment.

The scanned data (incoming correspondence regarding other health insurance submitted by beneficiaries and beneficiary representatives) is sent to the CMS Medicare Secondary Payer Systems to upload into their system, at which point the data in Benefits Coordination and Recovery Center becomes tagged for destruction.

Describe any agreements in place that authorizes the information sharing or disclosure.
The Benefits Coordination and Recovery Center data is only shared with the Medicare Secondary Payer Systems Contractor (MSPSC), which is also under the same overarching program (Coordination of Benefits and Recovery) and managed by the same CMS Business Owner. There is a Joint Operating Agreement between the two parties. The BCRC also has a Data Use Agreement (DUA) which includes all of the MSPSC systems. There are no agreements in place for the sharing and disclosure of PII with the beneficiary's attorneys, representatives, employer and insurer as these parties are all supporting the beneficiary and the primacy of payment.

Describe the procedures for accounting for disclosures.
A CMS approved standard operating procedure governs all disclosures. All disclosures are tracked within the MSPSC systems. A Joint Operating Agreement (JOA) between the BCRC and MSPSC is maintained that describes the responsibilities of each party for the sharing of information. The DUAs record who the PII is being shared between, for what purpose, and at what time it was shared. Inappropriate disclosures are reported to the BCRC Compliance Office, who in turn notifies the Department of Health & Human Services (HHS).

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 consent of PII collection is implied when contacting the BCRC Call Center. Collection of PII is inherent in the call process. If the caller does not provide PII, the BCRC is unable to provide service.

The outgoing questionnaires includes a Privacy Act statement as well as the purpose for which requested data is being 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.
The BCRC cannot provide services without PII being provided. Whenever individuals contact CMS for assistance, they always have the right to decline to give any personally identifiable information. However, without such information, in some instances, CMS' assistance may be limited.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.
Notification of a major change to the BCRC system that would impact the PII collected would be published in the applicable revised system of record notice(s) (SORN). The revised SORN is published in the Federal Register for a 60 day comment period by the public. Individual notification is not possible due to the nature of the BCRC 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.
If an individual has concerns that their Personally Identifiable Information (PII) is inaccurate, the individual may call the Benefits Coordination and Recovery Center (BCRC) Call Center. The BCRC staff can assist in routing the inquiry to the appropriate application representative in order to update the PII in that applicable CMS system. If the individual's concern is regarding inappropriately obtained, used, or disclosed PII, he/she may contact the Department of Health & Human Services (HHS) Office of Civil Rights (OCR).

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 Benefits Coordination and Recovery Center (BCRC) system is a pass through for data. There is no periodic review of the PII. The phone recordings and scanned image are for quality assurance purposes only. The Benefits Coordination and Recovery Center (BCRC) does not perform periodic reviews of Personally Identifiable Information (PII) because the BCRC system does not retain the data. Input validation is performed on data collected to ensure accuracy and relevancy before the data is sent to another CMS system.

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

Users:
The scanning staff is able to view the PII in the system in order to perform quality assurance of the scanned images.

Administrators:
The administrators can view the PII in the system to troubleshoot system issues.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.
Access requests require help desk tickets that must be approved by a CMS Group Director prior to acces being granted. System access levels are controlled at the application level. Users are assigned rights specific to those required for them to perform assigned job tasks.

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.
All access is limited to authorized staff and requires multifactor authentication to the network. Roles are assigned to individuals and access is granted for each application based on job function. The access granted is the minimum necessary required for the job.

Administrators have the ability to read and write PII. Users of the call recording application can only read/listen to PII and users of the image scanning software can read PII.

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.
BCRC staff, CMS employees and CMS contractors, take the CMS Computer Based Training (CBT) Security and Privacy Awareness training, which is required upon hire and annually thereafter.

Describe training system users receive (above and beyond general security and privacy awareness training).
System users are required to acknowledge Rules of Behavior (ROB), which are based on the Department of Health and Human Services' RoBs. All systems users also recieve role based training.

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.
For Medicare Secondary Payer (MSP) source documents (original incoming letters, checks, etc.), General Records Schedule (GRS) 3.2, Item 1, Disposition Authority: N1-440-01-05 states: destroy once the originals are scanned and verified, and a quality assurance process has been completed. The Benefits Coordination and Recovery Center (BCRC) retains the MSP paper files for up to 120 days.

The call recordings are kept up to 6 months for quality assurance purposes according to General Records Schedule 3.2, Item 3, Disposition Authority: N1-440-10-6. Destroy 3 months after the date of the incoming correspondence, or when no longer needed for Agency business, whichever is longer.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.
The Benefits Coordination and Recovery Center (BCRC) follows the CMS Information Security Acceptable Risk Safeguards for moderate impact level data systems, which includes administrative, technical, and physical controls.

Administrative: The BCRC system has a security plan and contingency plan. All users are trained on security awareness, privacy, and rules of behavior upon hire and annually thereafter.

Technical: The servers are built to a standard build and the configuration is monitored. The system is scanned for vulnerabilities and the vulnerabilities are remediated. Users are given least privilege and there is separation of duties.

Physical: Physical security to data centers is controlled through guards and proximity cards. Access to the racks is via key and/or biometrics. There is video surveillance in the data centers as well.

All controls are tested within a 3 year period as part of annual Federal Information Security Management Act (FISMA) evaluations