US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/26/2016

OPDIV:

CMS

Name:

Recovery Management and Accounting System

PIA Unique Identifier:

P-6508647-655166

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.

The application was migrated to a new data center.

Describe the purpose of the system.

The purpose of the Recovery Management and Accounting System (ReMAS) is to identify and track cases of mistaken and conditional payments that are to be recovered by the Centers for Medicare and Medicaid Services (CMS). ReMAS provides case creation and tracking, letter generation, and a standard reporting capability. Core functions: 1) to identify Medicare Secondary Payer (MSP) debt in a more timely manner, 2) to manage and control Medicare Secondary Payer (MSP) recovery cases in a centralized database, and 3) to be the system of record relative to the status of recovery of MSP claims by Medicare.

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

ReMAS utilizes beneficiary information stored within the application and contains the following types

of information: Social Security Number (SSN), Name, Phone, Taxpayer ID, Date of Birth, Mailing Address, Medical records Number, HICN, providers, suppliers, insurers, employers, attorneys and Employment Status. This information is used to support the collection, management and reporting of other insurance coverage of Medicare beneficiaries and the collection of conditional payments or mistaken primary payments related to Medicare claims.

ReMAS collects user ID and passwords and these login credentials are used to grant access to the system. Users of ReMas are the internal system administrators, maintainers and developers, and direct contractors. The login credentials (user ID) used to access ReMAS are provided to users by another CMS system, Enterprise User Agreement (EUA) which has its own PIA. EUA authenticates and approves requested ReMAS job codes.

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

If Medicare makes a mistaken/conditional primary payment in such a situation, Medicare pursues recovery of the mistaken primary payment from an appropriate party. Appropriate parties include providers, suppliers, insurers, employers, attorneys and beneficiaries. Once identified, the mistaken primary payments are considered debts to the United States and accounted for on that basis in Medicare's accounting system and financial statements. ReMAS identifies instances where Medicare made a mistaken or conditional primary payment when it should have been the secondary payer. Claims are then identified and put into cases for the applicable debtor.

ReMAS obtains identifying information about beneficiaries that should have been covered under another insurance. Claim information for those beneficiaries is also obtained so that users of ReMAS can identify whether each specific claim paid by Medicare was a mistaken or conditional payment that needs to be recouped.

Identifying information about providers, suppliers, insurers, employers and attorneys is also captured because that information is needed in order to develop a demand letter to the appropriate party.

Login credentials are used to grant access to the system. Users of ReMas are the internal system administrators, maintainers and developers, and direct contractors.

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 Records Number

Employment Status

Taxpayer ID

Other - User Credentials, (user ID, and password)

HICN's are collected

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

Employees

Public Citizens

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

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The primary purpose of the Personally Identifiable Information (PII) is to identify and track cases of mistaken and conditional payments that are to be recovered by CMS. For user credentials, the primary purpose is to log into the system for system support.

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

NONE

Describe the function of the SSN.

Occasionally the Social Security Number (SSN) is used to search for a beneficiary's case if the Health Insurance Claim Number (HICN) is unknown for the purposes of gathering claim information and to recover mistaken primary payments when another entity is responsible for primary payment.

Cite the legal authority to use the SSN.

The collection of this information is authorized by 42 U.S.C. 1395y (b) (7) & (8). The information collected will be used to identify and recover past mistaken Medicare primary payments and to prevent Medicare from making mistakes in the future for those Medicare Secondary Payer situations that continue to exist.

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

Title XVIII of the Social Security Act (The Act) (42 United States Code (U.S.C.) 1395kk(a) and 1395ll Sections 131(a), 1124, 1124A, 1173, 1175, 1816, 1834(j), 1842, 1842(r), 1874, 1874 (a), 1875, 1876, 1880, 1881(c)(7), 1902(a)(4)(A), 1902(a)(6), 1902(a)(25), 1902(a)(27), 1902(a)(49), 1902(a)(59), 1903(r)(6)(H)

The Economy Act of 1932 as amended (31 U.S.C. 1535 and 1536) is the authority with respect to other Federal agencies.

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.

09-70-0536, Medicare Beneficiary Database

09-70 -0008, National Provider System

09-70-0558, National Claims History

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

NONE

Is the PII shared with other organizations?

Yes

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

Other Federal Agencies

Shares data with the Department Of Justice (DOJ) for the purpose of recovering monies due to the Trust Fund.

Private Sector

Shares data with Medicare Secondary Payer Systems Contract (MSPSC) for the purpose of recovering monies due to the Trust Fund.

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

ReMAS has several electronic interfaces with other systems. Beneficiary data will be obtained from the Medicare Beneficiary Database
(MBD). Claims data are obtained from National Claims History (NCH) and National Medicare Utilization Database (NMUD) via the Data Extract System (DESY). Provider data will be obtained from the Online Survey, Certification, and Reporting (OSCAR), National Provider Identifier (NPI) and Streamlined Technology Acquisition Resources for Services (STARS) systems. Memorandums of Understanding (MOU)/Data Use Agreements (DUA) between ReMAS and all other interfacing systems have been established. This includes the Medicare Secondary Payer Systems Contract and the MOU between Office of Financial Management/Financial Services Group/Coordination of Benefits & Recovery (COB & R) and Office of Financial Management/Financial Services Group/Healthcare Integrated General Ledger Accounting System (HIGLAS).

Describe the procedures for accounting for disclosures.

Review of the Interconnection Security Agreement (ISA) between business partners are reviewed and tested annually. The CMS Privacy Office keeps an accurate account of disclosures though the use of the Data Use Agreement (DUA). The DUA captures Date, Nature, and purpose of the disclosure as well as the Name and address of the requesting person/agency. CMS currently retains the DUA over the life of the record. Providers can request disclosures of PII information from CMS.

Per language in the Interconnection Security Agreements (ISAs), parties are required to report privacy breaches or suspected breaches to CMS within one (1) hour of detection.

Disclosure of privacy information between systems is managed under routine use notices. In addition, system logs maintain transaction information only (not the PII itself) as a record or accounting of each time it discloses information as part of routine use.

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

ReMAS does not collect PII directly from the individual about whom it pertains. The information is supplied by other CMS systems of record. Those systems, MBD, NCH and NPS have processes in place to notify individuals that their PII will be collected. They have their own PIAs.

ReMAS also collects user ID and password from internal users in order to log into the system. However these login credentials (User Id and Password) are provided to users by another CMS system which is EUA. User accounts need to be created in EUA first before they can be granted access to ReMAS. The EUA PIA provides the process that notifies individuals that their personal information will be collected.

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 their Personally Identifiable Information (PII) because this information is needed to collect money owed to CMS.

Potential users cannot 'opt-out' of providing login credentials (user ID and Password). The login credentials are needed to grant access to ReMAS.

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

The PII within this system is provided through interconnections with other CMS systems which are documented within the DUA and is not collected directly from the individuals. In the event of a major change, the System of Record Notice (SORN) will be updated and posted on the HHS website to inform the public. This system contains Protected Health Information as defined by Health and Human Services (HHS) regulation "Standards for Privacy of Individually Identifiable Health Information" (45 CFR Parts 160 and 164, 65 FR 82462 (Dec. 28, 00), as amended by 66 FR12434 (Feb. 26, 01)). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the "Standards for Privacy of Individually Identifiable Health Information."

The login credentials within this system are provided to users by another CMS system which is EUA which has a PIA addresses the process to notify and obtain consent from the individuals.

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.

The beneficiary would contact CMS, who would in turn follow their Standard Operating Procedure (SOP) for processing beneficiary concerns / complaints. In accordance with the Medicare Beneficiary Handbook, individuals can use the following resources to resolve any concerns as they pertain to PII:

Visit Medicare.gov

Call 1-800-MEDICARE (1-800-633-4227) and
ask to speak to a customer service representative about Medicare’s privacy notice. TTY users should call 1-877-486-2048 or file a complaint with the Secretary of the Department of Health and Human Services. Call the Office for Civil Rights at 1-800-368-1019. TTY users should call 1 800 537 7697.

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 PII within this system is not collected by the ReMAS application. The PII is collected from the individual by other CMS systems and those PIAs should reflect how this process is addressed.

The Centers for Medicare and Medicaid Services (CMS) has a National Institute of Science and Technology (NIST) compliant continuous monitoring program to ensure system integrity, availability. The ReMAS system is designed with logic checks to ensure data accuracy and integrity. Yearly testing of the system is required to review and update data collection process to ensure data collected is relevant and accurate. Back-up servers are in place to ensure information is readily available, even if a main server fails.

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

Users:

The user uses the data stored in the system to associate claims to beneficiaries for the purposes of gathering claim information and to recover mistaken primary payments when another entity is responsible for primary payment.

Administrators:

The Administrators maintain the system to ensure data Confidentiality, Integrity and Availability.

Developers:

The developers performs development efforts pertaining to the system including troubleshooting and to resolving problems.

Contractors:

Direct contractors use the data stored in the system to associate claims to beneficiaries for the purpose of gathering claim information and to recover mistaken primary payments when another entity is responsible for primary payment.

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

Users, Administrators, Developers, and Contractors (direct) having system access are screened by their respective Human Resources (HR) departments. Roles are assigned based upon "need-to-know" or "need-to-access" requirements to perform their assigned duties. Technical security requirements include but are not limited to: user accounts, passwords, access limitation, reset procedures, suspension requirements, auditing procedures, and authenticator requirements.

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 ReMAS ISSO to identify abnormal activities if any.

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.

Access to PII is provided on a need to know basis based upon the principle of least privilege. This involves a separation of duties based upon each individual’s role.

Users: Different roles are defined at the user level based on a need to know. Differences in these roles include team/staff membership, access to the notices of settlements, access to checks/refunds, access to conditional payment letters, exhaust letters. The function that the user provides must be justified and go through an approval process before access is granted.

Developers: Developers are only given access based upon project and function (i.e. the ability to approve changes versus move changes). The function that the developer provides must be justified and go through an approval process before access is granted.

Administrators: Administrators are given access based upon project and function. Administrator roles are defined based upon the type of device/technology administered (i.e. windows admin, network admin, database admin, etc.) and are given access on an as needed basis. The function that the contracted individual provides must be justified and go through an approval process before access is granted.

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 employees who support the information system are required to complete privacy and security-based training prior to gaining initial access to the system and on a yearly basis thereafter. The following topics are the following: Information Security Awareness CMS/HHS Rules of Behavior Culture of Responsibility (Securing of all sensitive information within an employee's possession while completing system related tasks) and HIPAA Privacy Training. General Dynamics Information Technology (GDIT) shall ensure that “all” active credentialed Users, which includes contractor employees, and all third party vendors, are provided and take the Information Security Awareness (ISA) training:

(i) before authorizing access to the system or performing assigned duties; (ii) when required by changes; and (iii) annually thereafter. In addition, non-employee sponsors are responsible for ensuring compliance with this policy by the non-employee they are sponsoring. The contractor Information Systems Security Officer (ISSO) may accept certification of training from other contractor Business Units. If approved, the contractor ISSO provides the training completion date in order to update the user’s records.

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

In addition to the Information Security Awareness training that all employees are required to complete, users of the system are also required to complete the following courses as part of their training; Rules of Behavior, Health Insurance Portability and Accountability Act (HIPAA) Privacy, Culture of Responsibility. Descriptions of each course are provided below.

Rules of Behavior Training: The HHS Rules of Behavior (HHS Rules) provides common rules on the appropriate use of all HHS technology resources and information for Department users, including federal employees, interns and contractors.

Health Insurance Portability Accountability Act (HIPAA) training: The purpose of this Privacy Training course is to 1) increase HIPAA awareness, 2) define requirements of the Privacy Rule, 3) communicate Privacy policies, 4) provide examples of how Privacy requirements impact operations, 5) identify organizational support contacts, and 6) foster and maintain a culture of integrity.

Culture of Responsibility: This training course is designed to make sure employees are aware of their responsibilities in assuring the protection of customer data that has been entrusted to them.

CMS employees and contractors with privileged access are required to complete role-based training at hire and annually thereafter, and meet continuing education requirements commensurate with their role. Other training avenues such as conferences, seminars and classroom training provided by CMS is available apart from the regular annual 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.

This process is performed by the Data Center that hosts the system. CMS adheres to data retention and destruction policies/procedures that closely follow National Archives and Record Administration (NARA) guidelines related to data retention and NIST guidelines related to data destruction. More specifically, MSPSC adheres to NARA general records schedule (GRS) 20. Below are the NARA guidelines followed for retaining PII.

DISPOSITION: Temporary. Cut off annually. Delete/destroy 5 years after cutoff, or when no longer needed for Agency business, whichever is later. (Disposition Authority: NARA'S GRS 3.2, item 1).

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

ReMAS is regularly assessed using the CMS Security Policies and Controls that includes administrative, technical, and physical controls. All controls are tested within a 3 year period as part of annual FISMA evaluations.

Administrative: Administrative controls define acceptable use of the system and support the technical controls. Training (i.e. awareness, role-based, security, etc.), passwords requirements (i.e. age, length, complexity), reset procedures, suspension requirements, auditing procedures, and authenticators requirements. The ReMAs system uses the principle of least privilege as well as a role based access control to ensure system administrators, and users are granted access on a "need-to-know" and "need-to-access" commensurate with their assigned duties.

Technical: The data in ReMAS is secured through application security at the user level provided on a need to know basis based upon the principle of least privilege. Access to specific sets of data has also been set up at the database and environment level. Technical security requirements include but are not limited to user accounts, passwords, access limitation.

Physical: Physical access is restricted to personnel that requires physical access to perform their job function. Physical requirements included but are not limited to automatic door locks, keycard for access, locked cages, and access logs are maintained on site.