US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/29/2016

OPDIV:

CMS

Name:

CM - Maximus

PIA Unique Identifier:

P-8810813-553003

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?

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 CM-Maximus information system is used by Maximus Federal Services (Maximus), a CMS direct contractor, in the performance of Medicare appeal services as a CMS Qualified Independent Contractor (QIC). QICs are responsible for conducting the second level of Medicare appeals of coverage determinations, and payment disputes related to Medicare Hospital Insurance (Part A), Medicare Advantage Plans (Part C), and Prescription Drug Plans (Part D). The adjudication services include: processing appeal requests, tracking appeal data, and responding to correspondence related to the appeal.

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

The CM-Maximus system contains beneficiary and provider information and system user information. The information on beneficiaries consists of name, address, telephone number, email address, Health Insurance Claim Number (HICN), optional legal documents, medical records and medical notes. Provider's information consists of name, address, phone number, and National Provider Identifier (NPI). Correspondence with appellants is also contained within the system.

Information on system users consists of names, usernames, and passwords.

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

The CM-Maximus system contains contact information and medical information about Medicare beneficiaries and contact information about Medicare providers. The information on Medicare beneficiaries and providers is obtained from the Medicare Appeals System (MAS), which is another CMS information system. MAS maintains its own PIA for the information collected, stored and shared within it. It also contains correspondence with beneficiaries and providers about the status of the Medicare appeal.

Maximus is a CMS direct contractor and only Maximus employees are system users. To access the CM-Maximus system, users provide their user ID and password to obtain access to the system. User credentials are maintained for as long as necessary.

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

Photographic Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Medical Notes

Legal Documents

Other - Health Insurance Claim Number (HICN), User name, Password, NPI

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?

Beneficiary and provider PII is used for the processing of second level Medicare appeals for Medicare Part A, Part C, and Part D. System user PII is used to allow access to the CM- Maximus system.

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

Not applicable.

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

Authority for information use and disclosure is given under Section 205 of Title II, Sections 1155 and 1156 of Title XI, Sections1812, 1814,1816, 1842, 1869, and 1872 of Title XVIII of the Social Security Act as amended (42 United States Code Sections 405, 1320c-4, 1320c-5, 1395d, 1395f, 1395h, 1395u, 1395ff, and 1395ii). Additional authority is given under the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (Public Law 108- 173).

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.

09-70-0566 Medicare Appeals System, published 12/14/2004 and updated 9/15/2006

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

Not applicable.

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.

The CM-Maximus system does not directly notify individuals that their personal information is being collected because the system uses personal information from the MAS system.
However, providers and beneficiaries are informed on the appeal request form that providing their information is voluntary but failure to provide all or part of the requested information may affect the determination of their appeal.

System users are notified as part of the employment process and to obtain access to the CM-Maximus system that their personal information is required.

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 beneficiary and provider PII is required for appeal processing and is received from the MAS system. If the appeals process requires individuals to verify the information in the MAS system, they are notified on the standardized processing letters that the information provided will be used to further document their appeal and that submission of the information requested is voluntary, but failure to provide all or any part of the requested information may affect the determination of the appeal.

System user credentials, PII, are mandatory for system access, so there is no option to opt-out.

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

System users would be notified of major system changes through internal corporate email and training.

Medicare beneficiaries and providers would find notification of any major changes to the MAS system, and affecting PII, through the updating or revision to the System of Record Notice (SORN) in the Federal Register.

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 system users have concerns about their PII, they would contact the Maximus IT help desk. The help desk would investigate the incident and provide direction to the user on if further action is necessary. Beneficiary and provider PII is obtained from MAS. That CMS system is responsible for resolving any concerns about the PII within it.

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 system uses data directly from the Medicare Appeals System (MAS) which is the appeals system of record.

The PII contained in the CM-Maximus system is routinely backed up to ensure availability. User PII is protected and can only be modified by system administrators and is regularly reviewed for relevancy and accuracy. The PII of beneficiaries is verified with the MAS for accuracy and relevancy at the time of appeal case creation and reviewed throughout the appeal process, maintaining the integrity of the PII.

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 process second level Medicare appeals.

Administrators:

Administrators have access to PII to support proper system operation. In addition, administrators need access to create, review, and manage system user accounts.

Contractors:

Direct contractors, in their roles as users or administrators have access to PII as described in those explanations above: to access the system to process appeals or support the system's operation and to create, review and manage employee user accounts.

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

The system has both discretionary access control (DAC) and role- based access control (RBAC) within our system. System users are granted the most minimal access level to complete their job duties. System administrators review accounts at least semi-annually. All user activities are logged and reviewed.

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.

The system restricts access to information based on each end user's role within the system. Employees are granted the most minimal access level to complete their job duties, thus limiting their access to minimal amounts of 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.

System users are required to complete the CMS Security and Privacy Awareness training provided annually as a Computer Based Training (CBT) course. All system users complete annual corporate security training. Individuals with privileged access must also complete role-based security training based on their job function.

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

Not applicable.

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.

The CM-Maximus system follows the CMS Records Schedule published in April 2015 that details the records retention policy for the MAS system on page 96 of the schedule. Data retention complies with the National Archives and Records Administration (NARA) Disposition Authority: N1-440-09-5 Item 1b, which states that records will be destroyed 10 years after cutoff or when no longer needed for CMS business.

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

The system's administrative security controls consist of policies and procedures including security training, role-based access permissions and regular review of access logs and activities.

The system's technical security controls consist of restricting access using user ids and passwords, and firewalls and intrusion prevention. Technical protection is also achieved through continuous monitoring for system usage and unexpected or malicious activity; the configuration of specialty hardware and the use of encryption, including full disk encryption of laptops and workstations.

The system's physical security controls consist of restricted access and environmental protections, which consist of protected cooling and power sources. Access to this area is recorded, and restricted only to authorized personnel with appropriate security clearance. Facility access is controlled using badge access card readers. Designated high security areas are only accessible to approved personnel.
Physical equipment and media are subject to documented handling procedures, including proper disposal and destruction as necessary.