US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

01/24/2017

OPDIV:

CMS

Name:

Medicare Exclusion Database

PIA Unique Identifier:
P-9842164-216790

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?
Yes

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 authorization and authentication for access to Medicare Exclusion Database (MED) online application have been migrated from CMS Individuals Authorized Access to the CMS Computer Services known as IACS to the new CMS Enterprise Identity Management (EIDM) application.

Describe the purpose of the system.
The purpose of Medicare Exclusion Database (MED) application is to maintain the list of individuals and businesses that have been excluded from participating in the Medicare Program during the period of exclusion. The application shares the excluded provider data with Medicare Contractors, Law Enforcement agencies and other CMS applications to prevent fraud, waste and abuse.

Describe the type of information the system will collect, maintain (store), or share.
The system collects the Excluded Provider information such as Name, Date of Birth, Social Security Number (SSN), Employer Identification Number (EIN) and Exclusion related data provided by the CMS Office of Inspector General (OIG).

Access control information is maintained and controlled within the CMS Enterprise User Administration (EUA) and Enterprise Identity Management (EIDM) systems.

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

The CMS Office of Inspector General (OIG) generates the List of Excluded Individuals and Entities who are excluded from participating in the Medicare Program. The Medicare Exclusion Database (MED) application receives the excluded provider information from OIG on a monthly basis and MED is responsible for adding new sanctions and updating the existing data. The data is shared with approved users using an online web application available at https://med.cms.gov and also as downloadable files through the CMS Managed File Transfer (MFT) application with various user communities such as Medicare Contractors, Law Enforcement Agencies, State Medicaid Agencies, and other CMS applications etc.

The access to the MED and MFT site is managed through CMS Enterprise Identity Management (EIDM) and access can be requested through the CMS Portal website https://portal.cms.gov/.

The System collects information such as; Name, Date of Birth, Social Security Number (SSN), Employer Identification Number (EIN) and Exclusion related data, provider sanctions, reinstatements, a list of MED users from EIDM, and the provider information from National Plan and Provider Enumeration System (NPPES). The excluded provider information from OIG is compared with the provider information from NPPES to ensure data quality and consistency.

At the end of monthly processing of sanctions and reinstatements data, the database is updated to provide the latest information about the excluded providers and also the downloadable files are made available that includes current month's sanctions, reinstatements, cumulative sanctions, cumulative reinstatements, and any waiver data.

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

Taxpayer ID

Other: National Provider Identifier (NPI) number; Employer Identification Number (EIN) and

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

Vendor/Suppliers/Contractors

No

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

The Personally Identifiable Information (PII) is used in the system to provide information to the Carriers, Fiscal Intermediaries, States, Payment Safeguard Contractors, Zone Program Integrity Contractor and Medicare Advantage Payers – to identify and refuse payment to the excluded providers.

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

The secondary purposes could include data for research purposes and statistical analysis.

Describe the function of the SSN.

To assist in uniquely identifying sanctioned or reinstated providers. Additionally the SSN is used for comparing the National Provider Identifier (NPI) number received from OIG with the NPI number listed in the National Plan and Provider Enumeration System (NPPES).

Cite the legal authority to use the SSN.

Sections 1128 A and B and 1156 of the Social Security Act give the Department of Health and Human Services (HHS) through the Office of the Inspector General (OIG) the authority to exclude certain individuals and entities from participation in the Medicare and state healthcare programs.

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

Authority for maintenance of this system is given under §§ 1128 A and B, and 1156 of the Social Security Act.

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.

09-70-0534 - Medicare Exclusion Database (MED)

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Other HHS OpDiv

Identify the OMB information collection approval number and expiration date

Not applicable.

Is the PII shared with other organizations?

Yes

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

Within HHS

The MED data is shared within HHS and used by the CMS Provider Enrollment Chain and Ownership System (PECOS) to check for the excluded provider and by the Integrated Data Repository (IDR) through One Program Integrity (One PI) to perform analysis of fraud, waste and abuse.

Additionally we shared data with Carriers, Fiscal Intermediaries, Payment Safeguard Contractors, Zone Program Integrity Contractor and Medicare Advantage Payers also use MED data to identify and refuse payment to the excluded providers.

State or Local Agencies

The State Medicaid agencies also use the MED data to verify the enrollment into the State Medicaid Program.

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

All MED users are required to have their name present in the Data User Agreement (DUA) before the access is approved. A Memorandum of Understanding (MOU) is executed for any System to System transfer of data.

Describe the procedures for accounting for disclosures.

Any disclosure is filed and stored in the DUA Office within Office of Enterprise Data and Analytics (OEDA). This CMS office keeps track of all DUAs and are assigned a DUA number for easier tracking which allows the DUA to indicate when a disclosure was provided, who it was provided to, for what purpose, and when the disclosure needs to be re- reviewed.

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 notice is given - the PII is initially obtained / disseminated to MED via OIG. Individuals do not provide MED with their PII.

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 method to opt-out. All of the sanctioned provider data and information comes from OIG. They provide MED with a Sanctions and Reinstatement files, and Team MED pulls off the data that is required to identify an excluded provider.

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

There is no notification or consent process. The MED application does not interact with or contact the individual whose PII is in the system when a major changes occurs to the system because the source of data is from the CMS Office of Inspector General’s List of Excluded Individuals and Entities(LEIE) application. This application is responsible for notifying and obtaining consent.

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 Individual or entity whose information is incorrect would have to work with the OIG to resolve any data issues.

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

MED files are run against the NPPES database on a monthly basis, during which PII is validated against the National Plan and Provider Enumeration System (NPPES) database (which has been verified with SSA).

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

Users:

The users of MED online application have access to PII in order to identify the individuals and business entities that are excluded from Medicare Program.

Administrators:

The database administrators and system administrators have privileged access to the systems to perform routine maintenance and upgrades for the operating system, databases and other supporting applications. As such these users have access to locations where the PII is stored.

Developers:

Developers are responsible for maintaining and adding new functionality to the application. Additionally, they are required to support CMS enterprise application changes/upgrades, perform problem resolution within MED application and testing the data and functionality.

Contractors:

Direct contractors perform the operation and maintenance tasks of the system. Additionally, they assist in running monthly data update process and performing data corrections.

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

MED application implements role-based security wherein the access roles are defined and approved based on the assigned duty and intended system use. The system users must complete the necessary forms to initiate the request for access. The request has to be approved by the Security Point Contact (SPC) and the CMS Government Task Lead. Once the request for access is approved, a ticket is opened with the system administration group to provision the access for the approved 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.

MED application implements logical access controls and procedures are established to ensure that only designated individuals can access the system. MED application uses specific roles for access based on the job duty and separate roles have been defined for Development, Validation and Production environments. Additionally, the security is implemented using CMS Enterprise User Administration (EUA), Enterprise Identity Management System (EIDM).

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 users of the MED system are required to take annual Information Security and Privacy Awareness training to ensure the protection of and secure handling of the information being collected and maintained.

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.

The excluded provider PII information in MED is saved permanently because MED system serves both current operational needs as well as long-term knowledge management requirements for preserving institutional history and facilitating research on historical data that related to current matters. However the PII information obtained from National Plan and Provider Enumeration System (NPPES) is kept temporarily and deleted each month.

National Archives and Records Administration (NARA) record schedule is N1-440-09-18, items 1a, 1b, and1c.

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

Administrative Controls:

The MED application implements all applicable CMS security controls to protect the PII. The implementation of controls is documented under System Security Plan (SSP), Contingency Plan (CP) and Risk Assessment (ISRA) plan. Various reviews are performed periodically, such as accounts review, application access log review, audit log review etc. to ensure data protection and compliance. Additionally, all employees and contractors who have access to PII data are required to take annual Security & Privacy Awareness Training.

Technical Controls:

MED application uses CMS Enterprise Identity Management (EIDM) system for access management. The application uses Multifactor authentication for access, implements role-based security and functionality, inactivity session time-out and maintains audit trial history.

Physical Controls:

The MED application is housed in a secured data center and uses physical controls such as Armed security guards, Identification Badges, Key Cards, periodic access review and Closed Circuit TVs.

Identify the publicly-available URL:

https://med.cms.gov

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null