US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/29/2016

OPDIV:

CMS

Name:

HIPAA Eligibility Transaction System

PIA Unique Identifier:

P-1895367-241429

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?

Existing

Does the system have Security Authorization (SA)?

No

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.

There have been no changes to the system since the last PIA.

Describe the purpose of the system.

The Health Insurance Portability and Accountability Act (HIPAA) Eligibility Transaction System (HETS) provides eligibility data to Medicare Providers, Suppliers, or their authorized billing agents for the purpose of preparing an accurate Medicare claim, determining Beneficiary liability or determining eligibility for specific services.

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

HETS data is collected from other CMS systems, Medicare Beneficiary Database Suite of Systems (MBD), Common Working File (CWF), Enrollment Database (EDB), and Medicare Advantage and Prescription Drug System (MARX). The data is processed by the system, and returned to the originating sources. Transaction logs used to record system activity and are maintained in a

database that is outside of the HETS system. The following list of data elements describes the information processed by HETS.

The HETS system collects and maintains all submitter IDs and their relationships with Medicare Providers and manage access to the HETS system.

Beneficiary Demographics:

Beneficiary Entitlement, First, Middle and Last Name, Suffix, Date of Birth, Address, Gender, Healthcare Insurance Claim Number, Address, City, State, Zip, Applicable Date, Medicare Entitlement Effective Date(s) for Part A and Part B
Inactive Part A/B Period dates for Unlawful circumstances (Incarceration, Deportation, or Alien Status)

Beneficiary Date of Death
Coverage status of Services ,non Covered Services Type Codes
Base Deductible Remaining Deductible
Beneficiary Medicare Advantage Enrollment Medicare Advantage Enrollment Date(s) Medicare Advantage Contract and Plan ID Prior Managed Care Organization ID –
Managed Care Organization Contract ID + Plan Benefit

Submitter ID and Provider relationship

Name
Phone number Email address
Legal business name
Medicare Provider's Name
Billing address
Physical address
Technical Representative Name
Provider National Provider Identifier (NPI) ID

Users of HETS are CMS employees and direct contractors. A user ID and password is collected by HETS. Enterprise User Administration (EUA) is the CMS system which
provides a HETS user ID and password in order to enter the system.

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

The HIPAA Eligibility Transaction System (HETS) receives beneficiary information from Medicare Providers, Suppliers or their authorized billing agents and analyzes that data to determine beneficiary deductible and co- insurance for eligibility for services requested. HETS processes the submitted beneficiary data including information identifying the beneficiary (Name, Date of Birth and Health Insurance Claim Number) and the type(s) of services received/to be received. HETS then returns information including the deductible and co- insurance of the beneficiary and/or the beneficiaries' eligibility to be reimbursed for the services requested.

HETS uses Submitter information. Submitters consist of third party vendors and clearinghouses. The information collected is submitter ID, Provider ID, and Submitter Provider relationship.

Users of HETS are CMS employees and direct contractors. A user ID and password is collected by HETS. Enterprise User Administration (EUA) is the CMS system which
provides a HETS user ID and password in order to enter the system.

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

Name

E-Mail Address

Mailing Address

Phone Numbers

Other - Health Insurance Claim Number, Submitter ID, User Credentials, Incarceration, Deportation,

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

Employees

Public Citizens

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

No

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 data is to allow providers to confirm patient enrollment in the Medicare program and receive information related to benefits needed to correctly bill claims. Sharing this information is also required by Health
Insurance Portability and Accountability Act (HIPAA) for all covered entities. Medicare, as a health insurance provider, is a
covered entity under the law and is required to support these inquiry/response transactions.

HETS system user's PII is used to access the system for normal operations and maintenance.

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

None

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

Section 101 of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003; 5 U.S.C 301, Departmental Regulations

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.

Medicare Advantage Prescription Drug System (MARx), 09-70-4001

Common Working File (CWF), 09-70-0526 Enrollment Data Base (EBD), 09-70-0502

Medicare Beneficiary Database (MBD), 09-70- 0536

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

OMB approval number:
OMB-0938-0960 - Expiration 05-31-2017

Is the PII shared with other organizations?

Yes

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

Private Sector

PII may be shared with Medicare active providers who are currently enrolled within Medicare programs in order to provide services to Medicare Beneficiaries.

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

Trading Partner Agreements (TPAs) must be in place between the third party vendors and clearinghouses and CMS.

Describe the procedures for accounting for disclosures.

All transactions submitted to the HETS system gets monitored through the HETS monitoring graphical user interface (GUI).

The helpdesk GUI tracking functionality captures the submitter ID which identifies who submits the transaction and the NPI who identifies which Medicare provider is requesting eligibility information.

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 practice in place to notify submitters
or, third party vendors and clearinghouses, of the collection of their personal information is through completion of the Trading Partner Agreement form. Third parties are aware that personal information is needed in order to participate in the program which is conveyed to them verbally by CMS program officials.

The process to notify beneficiaries and providers lies with the systems who are the direct collectors of the PII. These systems are MBD, EDB, MARx and CWF and they each have a PIA.

The process in place to notify internal users of the HETS system that their PII is being collected is through the source collector, EUA. Requesting access to any CMS system, including HETS, through EUA ensures that a privacy statement has been supplied to users explaining why and how their information will be used.

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.

Submitters have the option to not submit their PII, however, they will not have be eligible to participate in the program.

The PII of beneficiaries and providers is collected by other CMS systems, MBD, EDB, MARx and CWF. The process lies with these systems which all have PIAs.

The PII collected from system users is required in order to perform their job duties therefore there is no process in place.

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

Third party vendors and clearing houses will be notified by the HETS helpdesk.

The CMS helpdesk will notify the system users if their user credential data will be collected or used differently.

Beneficiaries will be notified via the MBD, EDB, MARx and CWF System of Record Notices. If changes occur to how the PII is being collected, used and/or disclosed the SORNs will be revised and published for a 30 day comment period before becoming finalized.

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.

CMS has a documented incident handling process in place that is carried out by the HETS helpdesk. It is utilized to report any type of mishandling of PII data of system users.

Furthermore, individuals whose information has been obtained by the System of Record (SOR) CWF can contact the system Director, Division of Systems Operations, Business Applications Management Group, Office of Information Services, CMS, Room N2– 08– 18, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The individual will need to provide identifying information in order to make searching for the record in question easier and prevent delay. The director will then assess the issue and respond within the defined processes of CWF.

Individuals whose information has been obtained by the System of Record (SOR) MBD can contact the system Director, Division of Enrollment and Eligibility Policy, Medicare Enrollment and Appeals Group, Center for Beneficiary Choices, CMS, Mail Stop S1–05–06, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The director will then assess the issue and respond within the defined processes of MBD.

Individuals whose information has been obtained by the System of Record (SOR) EDB can contact the system Director, Division of Enrollment & Eligibility Policy, Medicare Enrollment and Appeals Group, Centers for Beneficiary Choices, Mail Stop C2–09– 17, Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244–1849. The director will then assess the issue and respond within the defined processes of EDB.

Individuals whose information has been obtained by the System of Record (SOR) MARx can contact the system Director, Division of Medicare Advantage Appeals and Payment Systems, Information Services Modernization Group, Office of Information Services, CMS, Room N3– 16–24, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. The director will then assess the issue and respond within the defined processes of MARx.

The subject individuals should contact the system manager named above, and reasonably identify the records and specify the information to be contested. 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.)

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

PII and PHI data submitted daily gets updated on a nightly basis: Lockheed Martin direct contractor and the Data Base Administrators run nightly updates to update the Integrated User Interface (IUI) database for Medicare beneficiaries' data eligibility. There are also backup tapes in order to ensure data availability.

The HETS TPA gets recertified in a yearly process, if it needs to be updated during the year, a full TPA must be resubmitted in order to ensure data relevancy and accuracy. The TPA is collected and maintained in the entry
tracking contractor tool.

Data integrity is protected by system user roles which only allow specific users to access the PII that is necessary to perform their job functions.

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

Users:

To determine if the beneficiary has Medicare Eligibility benefits to render services to the patient.

Administrators:

Application Support Activities including managing system users, auditing user access and providing support to users.

Developers:

Application Support Activities including developing code, maintaining code and testing the functionality of the system prior to promoting code to production.

Contractors:

Direct Contractors are developers and independent code testers and maintain code and test the functionality of the system.

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

Access is restricted on a least privilege and need to know basis and is certified yearly in line with CMS Security Requirements.

Requests for access are reviewed by HETS authorized officials at CMS to ensure only approved individuals maintain access consistent with their job responsibilities.

In the event an employee is terminated the GTL will take immediate action to remove access of the direct contractor immediately.

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 to the HIPAA Eligibility Transaction System (HETS) controlled by the EUA user ID and job codes associated with access to the HETS system.

We monitor the access of the system on a weekly basis to ensure they only access the minimal access necessary to perform their job.

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 system owners, managers, operators and contractors of the HIPAA Eligibility Transaction System (HETS) are required to have a CMS Enterprise User Administration (EUA) ID. As such, they are required to complete annual CMS Information Security and Awareness training (Computer Based Training). This training covers privacy and security controls for accessing any CMS system and, if not taken, the user's ID will be revoked until the training is completed.

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

N/A

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.

Personally Identifiable Information (PII) for system access information complies with National Archives and Record Administration (NARA) disposition: Cut off at the close of the calendar year. Destroy/delete 6 years and 3 months after cutoff. (NARA Disposition Authority: N1- 440-04-3, Item 1a)

PII is only maintained in system logs which are maintained and archived for 90 days in a database outside of the HIPAA Eligibility Transaction System (HETS). The process surrounding retaining and destroying the data associated with these logs is performed by the Baltimore Data Center, whose controls are regularly reviewed as required by CMS security requirements through the Federal Information Security Management Act (FISMA) Security Control Assessment (SCA) process.

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

HIPAA Eligibility Transaction System (HETS) resides in a government facility protected by security guards and is only logically accessible to registered personnel after undergoing extensive background checks, vetted, and approved. Technical controls include access controls which are established to limit system access to approved end users and operations/maintenance staff with a valid need to know and commensurate to their role. All policies relating to information security are addressed in the CMS organizational security and privacy policy and procedures, which all staff acknowledge upon hire and annually thereafter. Included in the policies and procedures are training for the proper handling of sensitive data as well as the minimum technical controls required for all federal systems to protect the confidentiality and integrity of data entrusted to CMS. HETS monitors system activity with the help of CMS to ensure PII is only used as intended for approved business requirements. Records are housed in both active and archival files in an encrypted format to protect data confidentiality and integrity.