US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/29/2017

OPDIV:

CMS

Name:

National Benefit Integrity-Medicare Prescription Drug Integrity Contractor

PIA Unique Identifier:

P-2815994-216790

The subject of this PIA is which of the following?

General Support System (GSS)

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.

N/A

Describe the purpose of the system.

National Benefit Integrity (NBI)-Medicare Prescription Drug Integrity Contractor (MEDIC), General Support System(GSS) is used to perform fraud and abuse investigation, support benefit integrity efforts, provide medical review support, national and regional data analysis, and law enforcement support. NBI-MEDIC (GSS) uses a variety of systems to perform its fraud and abuse investigation functions using the received claims, beneficiary, and provider data for Medicare. All of these systems run on data centers. The primary systems used on a day-to-day basis include the Health Information Tracking System (HITS) and the Common Working File (CWF) System.

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

NBI-MEDIC GSS receives claims, beneficiary, and provider data for Medicare. The information is used to detect and prevent fraud, waste, and abuse in the Medicare Fee For Service (FFS) program.

CLAIMS and BENEFICIARY data may include name, address, telephone number(s), Date of Birth (DoB), Medicare Number, Social Security Number (SSN), Health Insurance Claim Number (HICN), Medicare and Secondary insurer identification information, Driver's License or State Identification numbers, e-mail address, medical notes, taxpayer ID, medical records number, device identifiers, employment status, state ID numbers, complaint information, case assignment, nature of the complaint.

Provider data may contain Owner/Employee names, addresses, HICNs, licensures, certifications, financial information (bank account numbers, property ownership) and National Provider Identification Number (NPI).

User credentials (last name and first letter of first name) and encrypted passwords are contained within the system and are used for identification and authentication of authorized users.

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

NBI-MEDIC GSS uses a variety of systems to perform its fraud and abuse investigation functions using the received claims, beneficiary, and provider data for Medicare. All of these systems run on data centers.The primary systems used on a day-to-day basis include Health Integrity Tracking System(HITS). The HITS Application is used to store beneficiary and provider records containing complaint information, case assignment, nature of the complaint, beneficiary name, date of birth, address, phone number, Medicare/Medicaid number, provider information, provider name and address, phone number, investigator name, investigator address, investigator phone number, investigating agency, risk value, user credentials, last name and first letter of first name of the users and encrypted passwords are contained within the system and are used for identification and authentication of authorized users. The system tracks the case through the investigative process and stores the investigation outcomes. Information is also collected from multiple systems of record including; 09-70-0553 Drug Data Processing System- DDPS; 09-70-0527 Fraud Investigation Database- FID; 09-70-4001 Medicare Advantage Prescription Drug System- MARX; 09-70-0500 Health Plan Management System- HPMS; 09-07-0536 Medicare Beneficiary - MBD; 09-07-0571 Medicare Integrated Data Repository - IDR; 09-07-0501 National Claims History- NCH; 09-07-0532 Provider Enrollment Chain and Ownership (PECOS), Common Working Files (CWF). A separate Privacy Impact Assessment for the systems noted are covered by Centers of Medicare and Medicaid.

The information from these systems is used for analysis. The information is retained permanently unless otherwise directed.

Overall, these systems collect and maintain claim, beneficiary, and provider information for Medicare fraud and abuse cases.

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

Driver's License Number

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Financial Accounts Info

Certificates

Device Identifiers

Employment Status

Taxpayer ID

Other: National Provider Identification Number, Health Information Claim Numbers, User Credentials

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

Employees

Vendor/Suppliers/Contractors

Patients

Other: Providers and Beneficiary

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The information is used to detect and prevent fraud, waste, and abuse in the Medicare Parts C and D programs.

Users Credentials are stored for identification and authorization for access to the system.

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

N/A

Describe the function of the SSN.

The function of the SSN in NBI-MEDI is to identify beneficiary and providers in order for the system to perform its fraud and abuse investigation analysis and functions.

Cite the legal authority to use the SSN.

The legal authority for the collection and maintenance of this system is given under the provisions of sections 1812,1816,1842, 1832,1833, 1842, 1842(a)(2)(B), 1861, 1862, 1862(a)(1) and 1874 of Title XVIII of the Social Security Act (The Act) (42 United States Code (U.S.C.) 1395u, 1395y(b), and 1395kk).

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

Sections 1107,1815,,1816,1833,1842,1872,1874,1877,and 1902 of the Social Security Act (Title 42) U.S.C sections 405,1306,107,1395g, 1395h,1395l 1395u 1395ii,1395mm, 1395nn, and 1396a)

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.

09-70-0501 National Claims History- NCH

09-70-0500 Health Plan Management System- HPMS

09-70-0553 Drug Data Processing System- DDPS

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Other Federal Entities

Identify the OMB information collection approval number and expiration date

NO OMB collection approval is needed because PII is not collected directly from individuals with whom the information pertains and an OMB approval is not applicable to user credentials

Is the PII shared with other organizations?

Yes

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

Within HHS

Designated employees and direct contractors for the purpose of fraud, abuse and waste investigations.

Other Federal Agencies

Department of Justice (DOJ) and the Office of Inspector General (OIG) for use in fraud, waste and abuse investigations

State or Local Agencies

State and local law enforcement for the purpose of fraud, abuse and waste investigations.

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

Data Use Agreement #16092 and ISA agreements with Office of the Inspector General (OIG) and Department of Justice (DOJ)

The Data Use Agreement (DUA) authorizes information sharing for the purposes that support the case study, research and investigations.

The Information Sharing Agreement states the responsibility and requirements in which the third party must adhere to for the collection and use of the information which is being shared.

Describe the procedures for accounting for disclosures.

Per Data Use Agreement # 16092, disclosures of information to the OIG/DOJ shall comply with the Privacy Rule and Privacy Act. To comply with the Privacy Act, the OIG/DOJ must make all data requests using the form entitled "Office of Inspector General, Office of Investigations Data Use Agreement" to enable the tracking of disclosures that are made to law enforcement and health oversight agencies.

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

Information is obtained directly from Medicare direct contractors, claims processing systems and from a tap file on the National Claims History(NCH) feeds. Medicare beneficiaries sign a privacy act notice when they become eligible for Medicare. This act informs them that information they provide to justify payments, will be used to determine the appropriateness of the payment. Notices and consents are provided to individuals whose data is in the Medicare sources that feed the MEDIC System through Federal Register System of Record notices.

Internal system users are notified when they request user access for the system.

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.

Information is obtained directly from Medicare direct contractors, claims processing systems and from a tap file on the National Claims History(NCH) feeds. Medicare beneficiaries sign a privacy act notice when they become eligible for Medicare. This act informs them that information they provide to justify payments, will be used to determine the appropriateness of the payment. Notices and consents are provided to individuals whose data is in the Medicare sources that feed the MEDIC System through Federal Register System of Record notices.

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

All PII information is obtained from the listed Systems of Record. Changes to the systems will be reflected in the System of Record notices.

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.

Disclosures of PII would be reported directly to the Computer Security Incident Response Team (CSIRT) according to the incident handling procedures.

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

NBI-MEDIC GSS utilizes several network monitoring tools to ensure data protection , integrity and system availability including system event monitoring and intrusion detection. Accuracy and relevance of the data is reviewed by the data analysis team.

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

Users:

To detect and investigate fraud and waste in the Medicare Parts C and D programs.

Administrators:

Administration of the GSS environment

Developers:

Development and maintenance of the GSS.

Contractors:

To detect and investigate fraud and waste in the Medicare Parts C and D programs.

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

User access is controlled via administrative and technical controls. A formal process is defined for account creation that includes limiting account categories to only appropriate resources. Account creation and modification of permissions must be requested by functional leadership. Reviews are conducted monthly to ensure the formal processes are being followed and to ensure that accounts that no longer need access are being removed.

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.

Users can only access networks allowed by their user profile. The user profiles dictate the level of access granted (user profiles define security groups that individuals are a member of). Users must be authenticated prior to gaining access, application and file level permissions are enabled to facilitate minimal access.

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.

User security awareness training is required prior to access being granted. Security awareness training includes attestation to a series of policies, procedures, and directives including Rules of Behavior. Training is required to be completed upon hire and annually thereafter. A system login banner is in place to be displayed prior to system access that specifies the requirements for protecting the information.

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

NBI-MEDIC direct contractors support/Health Integrity direct contractors receive job specific training which include the specific systems to be accessed. The training includes peer training, slide presentations, manuals and guides, and work instructions. Training is conducted at least once a year and whenever the need for supplemental or new training arises.

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.

NBI-MEDIC direct contractor support/Health Integrity has a policy for handling sensitive information and storage and destruction. For hard copy sensitive data, locked recycle bins are placed in designated locations. These bins are used to discard documents or papers with Personally Identifiable Information (PII) and/or confidential data or information. The company's contracted vendor comes to empty recycle bins and shreds the contents on-site. Backup tapes from the system are stored in a secured offsite facility . All tapes are considered sensitive (may contain Protected Health Information (PHI/PII) and are tracked from initial use through to disposal using bar-code labels which are scanned by both the backup operators, as they move from Data Center to vault, and by the destruction vendor. The destruction services is in accordance with NIST SP 800-88 Guides for Media Sanitization. National Archive Records Association (NARA) record retention schedule citation number is (Disposition Authority: N1-440-04-3, Item 1a) Hardcopy Records - The hardcopy must be retained onsite until the microform has been verified. Cut off at the close of the calendar year in which paid; transfer hardcopy to a Federally-approved records storage facility only if there is a corresponding master microfilm record that can be retained for the period indicated in b. below; otherwise, the hardcopy shall be retained until the 6 years and 3 months period is reached. Earlier cutoff and transfer is authorized. However, the hardcopy must be retained for a total retention of 3 years after the close of the calendar year in which paid.

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

Physical access controls include; a visitor access policy - visitors must be signed in and escorted, employees must wear ID badges, access to secure areas is controlled by proximity card, areas storing PII are limited to necessary staff, physical intrusion detection is in place (alarm system), cameras are in place within the primary location that hosts the data center, the data center is equipped with redundant air conditioning, redundant power, a gas based fire suppression system, and environmental monitoring (temp, water, power loss).

Technical controls include; a firewalled enclaved network specific to the contract, encrypted connectivity into and out of the encrypted enclave (FIPS 140-2), network access control, host based intrusion detection, network based intrusion detection, system event monitoring, centralized security patch management, access control policy and procedures (account management - access limited by user profile, all access is monitored), Active Directory (to facilitate access control), file level permissions based on required access, routine system vulnerability scanning, centralized anti-virus and malware management, whole disk encryption (for laptops used off site), RSA dual factor authentication (for users working off site)

Administrative controls include; User security awareness and Rules of Behavior training (required prior to granting access), a change advisory board (CAB) (to facilitate system changes), a fully maintained System Security Plan, a yearly FISMA assessment (for the required 1/3 controls), Security Control Assessments are performed (initially and every 3 years thereafter), a Risk Assessment is documented and reviewed annually.