US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/06/2017

OPDIV:

CMS

Name:

Zoned Program Integrity Contractors Zone 4 - HealthIntegrity

PIA Unique Identifier:

P-6258296-214190

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.

No changes have occurred.

Describe the purpose of the system.

The Zoned Program Integrity Contractor (ZPIC) for Zone 4 is used to collect and analyze operational data from Medicare contractors across the country for use in detecting and preventing fraud, waste and abuse (FWA) as well as abuses within the Medicare Part A, B and D programs and the Medicaid and Hospice programs. Information is also used in the Texas Medicare Medicaid Data Match project. (Medi-Medi). The purpose of the Medi-Medi program is to detect fraud, waste and abuse in the state of Texas. This program incorporates data mining, coordination and data sharing to identify fraudulent and wasteful billing behavior that goes undetected when programs are being reviewed in isolation.

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

The Zoned Program Integrity Contractor (ZPIC) for Zone 4- Health Integrity General Support System (GSS) receives claims, beneficiary, and provider data from Medicare, Medicaid and Hospice. The information is used to detect and prevent fraud, waste, and abuse in the Medicare/Medicaid Fee For Service (FFS) program. CLAIMS and BENEFICIARY data may include name, gender, address, telephone number(s), Date of Birth (DoB), Medicare Number, Medicaid Number, Health Insurance Claim Number (HICN), Medicare and Secondary insurer identification information, drivers license or state identification numbers, social security numbers (SSN), medical record numbers and tax ID numbers. PROVIDER data may contain owner/employee names, addresses, HICNs, licensures, certifications, financial information (bank account numbers, property ownership), tax ID number and relationships with other entities within their group.

User Credentials consisting of user ID and password are maintained within Active Directory within the secured ZPIC contract network. System administrators and users, including CMS direct contractors and other private sector contractors are required to use multi-factor authentication to access data based on their role and group policy assigned to that role, based on their business needs.

The following systems, which have their own PIAs, are used to pull information to be used in the ZPIC 4 program.

National Claims History (NCH) 09-70-0558

Common Working Files (CWF) 09-70-0526

Medicare Drug Data Processing System (DDPS) 09-07-0553

Enrollment Database (EDB) 09-70-0502

Fraud Investigation Database (FID) 09-70-0527

Health Plan Management System (HPMS) 09-70-0500

Intern and Resident Information System (IRIS) - 09-70-0524

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

Medicare Beneficiary Database (MBD) 09-70-0536

Medicare Exclusion Database (MED) 09-70-0534

National Provider System (NPS) 09-70-0008

Provider Enrollment Chain and Ownership System (PECOS) 09-70-0532

Medicare Retiree Drug Subsidy Program (RDSP)- 09-70-0550

HHA Outcome and Assessment Information Set (OASIS) 09-70-0522

Medicare Integrated Data Repository (IDR) 09-70-0571

One ProgramIntegrity Data Repository (OnePI) 09-70-0568

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

The Zoned Program Integrity Contractor (ZPIC) for Zone 4- Health Integrity General Support System(GSS) uses a variety of systems (NCH, CWF, EDBRDSP, IDR, OnePI, PECOS, MBD, DDPS, MARx, FID, HPMS, IRIS, MED, NPS, OASIS) to perform its fraud and abuse investigation functions. It uses the claims, beneficiary, and provider data received from these systems for Medicare, Medicaid and Hospice FWA analysis. The primary applications used on a day-to-day basis include the SAS (Statistical analysis Systems) and Zeus. Health Integrity is the maintainer/data warehouse of the SAS and ZEUS applications. The information that is housed in the data warehouse are Hospice, Medicare and Medicaid claims in the jurisdiction that have been processed. Queries are run using Business Objects or the current version of Suite of Analytics Software (SAS) provide Claims Histories, Provider Profiles, Peer Comparisons, Average Billing Reports and statistically valid random samples that contain beneficiary PII, PHI and claims data. The Zeus application is the internal case management system. It allows for the Analyst/Investigator to track their cases and keep a history of the progression of the case. Maintaining a case tracking system is a Centers for Medicare and Medicaid Services (CMS) contract requirement. Overall, these systems collect and maintain claim, beneficiary, and provider information for Medicare fraud and abuse cases.

System user credentials are collected for authentication to the system in order to perform analysis duties.

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

Financial Accounts Info

Certificates

Legal Documents

Employment Status

Taxpayer ID

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

Employees

Public Citizens

Vendor/Suppliers/Contractors

Patients

Beneficiaries and physicians

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

PII is used to search for information on beneficiaries, claims and investigation information pertinent to analyzing data for detection of fraud, waste and abuse. User PII is used for authentication to the system in order to support the system functions.

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

Not applicable

Describe the function of the SSN.

Social Security Numbers are used to verify the identity of providers and beneficiaries, in an effort to combat fraud, waste and abuse of federally funded healthcare benefits and programs.

Cite the legal authority to use the SSN.

Legal authority is given under the provisions of sections 1816, 1842, 1862(b) and 1874 of Title XVIII of the Social Security 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.

Authority for the collection and maintenance of this system is given under the provisions of sections 1816, 1842, 1862 (b) and 1874 of Title XVIII of the Social Security Act (The Act) (42United States Code (U.S.C.) 1395u, 1395y (b),and 1395kk).

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.

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Other Federal Entities

Non-Governmental Sources

Private Sector

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

For use within fraud, waste and abuse investigations

Other Federal Agencies

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

State or Local Agencies

State and Local Law enforcement for use within fraud, waste and abuse investigations

Private Sector

Private sector contractors to provide assistance in medical reviews on behalf of Health Integrity.

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

There is a Data Usage Agreement (DUA) which authorizes the contractor to receive information from the CMS Systems of Record listed above for the purpose of supporting the case study, research and investigative projects set forth by CMS.

Describe the procedures for accounting for disclosures.

Information disclosure logs are kept for all data that is sent outside of the system. Logs include PII disclosed outside of the system. Log records indicate to whom the PII is disclosed (or why the record does not indicate); reason for sharing the PII, collected or maintained in the system, or shared with another system, (or why the record does not indicate).

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

Notices and consent are provided to individuals whose data is in the Medicare sources that feed the ZPIC System through the Federal Register System of Record (SOR) Notices: 09-70-0568 One Program Integrity Data Repository (OnePI) and 9-70-0527 The Fraud Investigation Database (FID).

There is no specific process to notify system administrators because they provide their user ID and password in order to perform their job duties.

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 contractor claims processing systems and from tap files on the NCH feeds. Medicare beneficiaries sign a Privacy Act notice when they become eligible for Medicare that informs them that the information they provide to justify payments will be used to determine the appropriateness of payment.

System administrators cannot opt-out of providing their PII as the user ID and password are used to log on to the system in order to perform their job duties.

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

No process is in place to notify and obtain consent from the individuals, whose PII is in the system, when major changes occur to the system because the system does not collect PII directly from individuals. The system collects PII from other systems.

System administrators will be notified via email communications when major changes occur to the system.

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.

No process is in place to notify and obtain consent from the individuals, whose PII is in the system, when major changes occur to the system because the system does not collect PII directly fromindividuals. The system collects PII from other systems.

System administrators can report any issues to the CMS Information Technology (IT) Service Desk and they will be resolved accordingly.

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

Records are reviewed and analyzed individually by trained case workers as part of the data analysis process. Validation edits are performed by the system to ensure data integrity.

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

Users:

To detect fraud, abuse, and waste in the Medicare Parts C and D program

Administrators:

Administration of the General Support System and IT environment

Developers:

Development and Maintenance of the major application used for case management (ZEUS)

Contractors:

To detect and investigate fraud, waste and abuse in the Medicare Parts C and D program. Contractors are used to assist in medical reviews. Some are HHS contractors and others are private sector. Those that are private sector are use to provide assistance in medical reviews on behalf of Health Integrity.

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

System and data access is determined by job function. Access is role-based and controlled by 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 permissions must be requested by functional leadership or Business Owners. Reviews are conducted monthly to ensure account reconciliation is being performed.

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 is role-based with least privilege, based on job functions. User profiles dictate the level of access granted (user profiles define the access level and security groups that the individuals are a member of).

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.

Users are required to complete CMS Security and Privacy Awareness training prior to accessing the system. This training is mandatory and completed annually. Attestations to the policies, procedures, directives and Rules of Behavior are required and signed.

All users are required to complete Ethics Training, Insider Threat training, and HIPAA training upon hire and annually thereafter.

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.

CMS has established processes and guidelines with regards to data destruction and retention. The PII stored within the system follows the National Archives and Records Administration (NARA) Records Control Schedule (RCS) # N1-440-09-015: DISPOSITION: TEMPORARY Cut off at the end of the Fiscal year (FY) Delete/Destroy 75 years after cutoff, and N1-440-09-4: DISPOSITION: PERMANENT Cut off annually Pre-accession files to the National Archives 5 years after cutoff Legally transfer individual files In an acceptable format (following current Code of Federal Regulations (CFR) guidelines) to the National Archives annually, 20 years after cutoff based on the system and PII data collected and stored.

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, 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), 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 Federal Information System Management Act (FISMA) assessment (for the required 1/3 controls), Security Control Assessments are performed (initially and every 3 years thereafter), Risk is assessed and documented and reviewed annually.