US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/16/2017

OPDIV:

CMS

Name:

Zoned Program Integrity Contractors - SGS

PIA Unique Identifier:

P-3535148-999646

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.

NONE

Describe the purpose of the system.

The Zoned Program Integrity Contractors - SafeguardServices LLC General Support System (ZPIC-SGS) is used to perform fraud (Over billing, inappropriate services, excessive services, etc.) and abuse investigation, support benefit integrity efforts, provide medical review support, national and regional data analysis, and law enforcement support.

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

The Zoned Program Integrity Contractors – SafeguardServices LLC General Support System (ZPIC-SGS) 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, Health Insurance Claim Number (HICN), Medicare and Secondary insurer identification information, Driver's License or State Identification numbers. Provider data may contain

Owner/Employee names, addresses, HICNs, licensures, certifications, financial account information (bank account numbers, property ownership), and relationships with other entities within their group.

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 Contractors – Safeguard Services LLC General Support System (ZPIC-SGS) uses a variety of systems using the received claims, beneficiary, and provider data for Medicare to perform fraud and abuse investigation, support benefit integrity efforts, provide medical review support, national and regional data analysis, and law enforcement support. All of these systems run on data centers. The primary systems that comprise the GSS, and are used on a day-to-day basis include the Workload Management Module (WMM), the Medical Review Case Tracker (MRCT), the Integrated Fraud & Abuse Detection System (IFADS), and the Common Working File (CWF) System.

The information types that are housed in the data warehouse are Medicare Durable Medical Equipment (DME) claims that have been processed, Home Health and Hospice, Fee for service claims, and inpatient and outpatient claims. Queries are run by SGS analysts and investigators using Business Objects or the current version of Suite of Analytics Software (SAS) provider Claims Histories, Provider Profiles, Peer Comparisons, Average Billing Reports and statistically valid random samples that contain beneficiary PII, PHI and claims data are reviewed by the SGS staff to identify potential waste, Fraud or abuse. The MRCT application is the internal case management system. It allows for the Analyst or 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 are populated with claim, beneficiary, and provider information obtained by SGS from CMS or other CMS Contractors, for use by SGS in identifying potential Medicare Waste, 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.

Date of Birth

Name

Driver's License Number

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Financial Accounts Info

Certificates

Other: State Identification numbers; (HICN) Health Insurance Claim Number, Medicare Insurance

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

Employees

Public Citizens

Patients

Beneficiary

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 Personally Identifiable Information (PII) use is for ensuring correct Medicare claim payment determinations. PII is also used to create user credentials for identifying users and providing them their proper user role access into the system.

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

N/A

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) (42 United 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.

09-70-503 (Intermediary Medicare Claims Records System - Routine Use 1)

09-70-501 (Carrier Medicare Claims Records System - Routine Use 1)

09-70-0527 The Fraud Investigation Database (FID); 09-70-0568 One Program Integrity Data

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

State/Local/Tribal

Other Federal Entities

Other

Identify the OMB information collection approval number and expiration date

N/A for user credential information

Is the PII shared with other organizations?

Yes

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

Within HHS

Centers for Medicare and Medicaid Services (CMS) and Office of Inspector General (OIG), for Medicare program payment safeguards oversight and ensuring correct Medicare claim payment determinations. Incorrect payments may result in Administrative Actions to include overpayment identification and collection, law enforcement fraud referral, civil and/or criminal monetary penalties

Other Federal Agencies

Department of Justice (DOJ) and Federal Bureau of Investigation (FBI), for law enforcement fraud referral, criminal prosecution, civil and/or criminal monetary penalties.

State or Local Agencies

Medicaid Fraud Control Units, Medicaid Program Integrity for program payment safeguards oversight and ensuring correct claim payment determinations. Incorrect payments may result in Administrative Actions to include overpayment identification and collection, law enforcement fraud referral, civil and/or criminal monetary penalties.

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

Memorandum of Understanding (MOU) between Centers for Medicare and Medicaid Services (CMS) & Health and Human Services Office of Inspector General (HHS OIG) & U.S. Department of Justice Federal Bureau of Investigation (DOJ FBI) that allows for provision of beneficiary and provider information for the purpose of investigation allegations of potential waste fraud and abuse

Describe the procedures for accounting for disclosures.

A Data Use Agreement is required from Law Enforcement for any requests for disclosure of Personally Identifiable Information (PII). These are maintained in the Medical Review Case Tracker, an internal case tracking system database maintained by The Zoned Program Integrity Contractors - SafeguardServices LLC General Support System (ZPIC-SGS) and in hard copy files. Medical Review Case Tracker keeps records of the law enforcement information requests, the requesters and their agencies alongside the specifics of their information request.

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

Notice is given to individuals whose data is in the Medicare system that feeds the Safeguardservices LLC GSS through Federal Register System of Record (SOR) Notices: 09-70-0568 One Program Integrity Data Repository (ODR) and 9-70-0527 The Fraud Investigation Database (FID). For users who are accessing the system, they are provided notice that their information will be collected should they request access to 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.

This system does not collect PII directly from individuals. That data collection is done prior to the data reaching this system. Centers for Medicare and Medicaid Services (CMS) employees cannot opt out because their info is necessary as part of their employment. If they choose not to provide their PII then they do not participate in the Medicare program.

Users of the system must also provide their personal identifiable information should they require to obtain access to the system.

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

The ZPIC-SGS does not have a process in place because it does not collect Personally Identifiable Information (PII) from individuals. However Centers for Medicare and Medicaid Services (CMS), through their Medicare Administrative Contractors, notifies individuals if there are Medicare program system changes. Notice occurs in Explanation of Benefit notices, Remittance Advices and through the Medicare Learning Network.

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 ZPIC-SGS does not have a process in place because it does not collect Personally Identifiable Information (PII) from individuals directly.

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 personally identifiable information (PII) contained in this system is not collected by this system, but is provided by other CMS systems for the purposes of performing analysis of the data provided to identify potential waste fraud and abuse activities. The system itself is a read only instance of the information and not an authoritative source for any purpose but analysis. Updates to the system are done by following the CMS Technical Reference Architecture(TRA) process as well as the CMS Acceptable Risk Safeguards(ARS) requirements. The system maintains test the data integrity, availability, accuracy and relevancy of the data by placing data is testing tables and then performing automated and manual data quality checks. Also, the information used to identify the individual and will provide them their proper user role in the system for the activities they are to perform in the system. The SGS internal systems are read only, and use replicated data from the Systems of record, since all information is a replica and not the authoritative data, Issues of confidentiality, availability, integrity and non-repudiation are mitigated.

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

Users:

In performance of analysis of the data contained in the system, and to identify potential instances of waste, fraud or abuse, the system users will have access to the PII in the system in order to detect fraud, abuse, and waste in the Medicare FFS program

Administrators:

The Administrators of the system have access to the information in the system to perform maintenance on the system, perform system audits, and maintain the system overall. Role based access is also set up where certain administrators that are assisting with the maintenance of the system will also have access to the information of the users of the the system to manage their access and audit their use of the system.

Developers:

Development and Maintenance of Major Applications as well as development of statistical analysis models requires access to the PII contained in the system to perform queries that help identify waste fraud and abuse in the program. Role based access is also set up where certain developers that are assisting with the maintenance of the system will also have access to the information of the users of the system.

Contractors:

In performance of analysis of the data contained in the system, and to identify potential instances of waste, fraud or abuse, the system users (direct contractors) will have access to the PII in the system in order to detect fraud, abuse, and waste in the Medicare FFS program.

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

SafeguardServices LLC has implemented a Segregation of Duties Policy. The SafeguardServices llc Internal Audit Department reviews the sufficiency of segregation of duties procedures through periodic audits. The first area of concern is the protection of sensitive information. Job assignments are analyzed by preparing a matrix of all positions. Physical and logical access controls help restrict employees to authorized actions, based upon organizational and individual job responsibilities. At least annually, or whenever major changes are made to the SafeguardServices llc organization structure, management performs a high level review of segregation of duties to ensure that new risks have not been created due to organizational changes or changes in assignment of duties within Medicare operations. Resources are classified based on risk assessments.

Classifications are documented and approved by an appropriate SafeguardServices LLC senior official and are periodically 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.

Every user of the system has a user account comprised of a unique identifier (User Name or Identification) as well as an account authenticator (password) that provides access to the system. Once the user has been authenticated (Approved for access based on username and password) and starts to perform analysis, the user would select a record, and the system would compare the record requested with the users authorization to determine if the user is allowed to access that record. This series of requirements is called role based access, and is defined for each type of user to ensure that users only have approved and appropriate privileges to information that they must access, and no other information.

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 personnel that interact with this system personnel (system owners, managers, operators, contractors and/or program managers) using the system are provided annual training to make them aware of their responsibilities for protecting the information being collected and maintained this annual training is monitored and tracked at the account level and includes internal application training, security and awareness training and developed desk level procedures.

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

All personnel (system owners, managers, operators, contractors and/or program managers) using the system are provided additional training, above the general security and privacy and awareness training on an annual basis. This Health Insurance Portability and accountability Act Training ensures that all participants are aware of their responsibilities for protecting the information being collected and maintained.

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.

No information is destroyed, all Information is retained off-site indefinitely at a secure storage facility that conforms to the NARA guidelines per N1-440-09-4, Item 1a, (Cutoff annually. Delete/destroy 10 years after cutoff), and all information and media is transported in accordance with the requirements for media protection as outlined in the CMS Business Partners System Security Manual and Acceptable Risk Safeguards.

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

The ZPIC system operates behind secure firewalls on the CMS WAN and is housed at physically secure sites. BPSSM and FISMA requirements are followed. A systems security plan details controls for the 17 FISMA families of controls. Controls include firewalls, IDS, network authentication, file based permissions, application level permissions; event monitoring, change control procedures, minimum system security standards (baselines/hardening); anti-virus, encryption, patch management; network level hardening (AD group policy). Physical security controls include visitor sign-in requirement, keycard requirement, physical intrusion detection, video cameras, employees must wear badges; perimeter doors are locked after hours; containers and rooms containing PII are protected by dual barriers (perimeter walls, interior walls or metal locked containers) and any data leaving data center must be encrypted.