US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/08/2017

OPDIV:

CMS

Name:

Fraud Prevention System

PIA Unique Identifier:

P-3834359-341274

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Requirements Analysis

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?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

CMS instituted the National Fraud Prevention Program (NFPP) by implementing a predictive modeling system capable of identifying high-risk claims and an integrated case management system. The Fraud Prevention System uses predictive analytics to identify troublesome billing patterns and outlier claims for action, similar to systems used by credit card companies. FPS uses the integrated case management system to manage the predictive modeling alerts inclusive of preventing the payment from being issued at time of initial adjudication.

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

The Fraud Prevention System maintains and stores information about Medicare beneficiaries and their claims, providers, and FPS system users who are internal CMS employees and direct contractors. The information maintained about beneficiaries and providers includes Name, email addresses, Phone Number, Date of Birth, Mailing Address, Medical Records Number, Health Insurance Claim Number(HICN), National Provider Identifier(NPI) and isreceived from the following other CMS systems which each have their own PIA:

CMS Shared Systems, Common Working File, Enrollment Database (EDB), Healthcare Integrated General Ledger Accounting System (HIGLAS), Integrated Data Repository (IDR), Medically Unlikely Edits System (MUE), Medicare Beneficiary Database (MBD), Medicare Exclusion Database (MED), National Claims History (NCH), National Fraud Investigation Database (FID), Provider Enrollment Chain and Ownership System (PECOS).
System user (internal system administrators and maintainers) information FPS collects is username and password in order to gain access to FPS to perform regular system operations.

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

The system monitors 4.5 million claims (all Part A, B, DME) each day using a variety of analytic models. FPS generates alerts that are consolidated around providers and subsequently prioritized based on risk. The results are provided to the Zone Program Integrity Contractor (ZPICs) analysts, Program Safeguard Contractors (PSCs) and investigators with views by regions.

The information collected about providers and beneficiaries is used to create profiles based on provider billings and beneficiary utilization patterns for the purpose of combating fraud, waste and abuse. As such, it is capable of reporting alerts based on risk scoring applied to near real-time claims. The results are available to CMS' Centers for Program Integrity (CPI) and law enforcement partners in a prioritized national view.

The case management tool within FPS manages the predictive modeling alerts and provides provider profile information and support to key stakeholders in their pursuance of suspicious provider billing patterns.

System user (internal system administrators and maintainers) information FPS collects is username and password in order to gain access to FPS to perform regular system operations.

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

Medical Records Number

Other: Health Insurance Claim Number(HICN), National Provider Identifier(NPI), System user and

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

Employees

Vendor/Suppliers/Contractors

Patients

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

The primary purpose of the FPS system in collecting PII is for fraud investigators to identify fraudulent claims before payments are made to providers.

CMS direct contractors including Medicare Administrative Contractors (MAC), CMS Enterprise Data Centers (EDC), Recovery Audit Contractors (RAC), Zone Program Integrity Contractors (ZPIC), Program Safeguard Contractors (PSC), and Common Working File (CWF) use the data, which includes PII, to investigate fraudulent claims.

The system utilizes the usernames and passwords of users to ensure authorized access to the system.

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

FPS ensures that PII is de-identified when practicable. FPS uses masked data for testing and training.

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

Section 4241 of the Small Business Jobs Act of 2010 (Public Law 111-240) mandates the use of predictive modeling and other analytic technologies to identify and prevent fraud, waste and abuse.

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.

09-70-0527 - Fraud Investigation Database

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 Federal Entities

Identify the OMB information collection approval number and expiration date

OMB collection approval number is not needed 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.

Other Federal Agencies

Office of Inspector General (OIG) and Federal Bureau of Investigations (FBI) in order to aid in investigation of fraud, waste and abuse.

State or Local Agencies

Law Enforcement in order to aid in investigation of fraud, waste and abuse.

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

CMS has Memorandum of Understanding (MOU) in place with the FPS direct contractors to provide information to other CMS direct contractors including Medicare Administrative Contractors (MAC), CMS Enterprise Data Centers (EDC), Recovery Audit Contractors (RAC), Zone Program Integrity Contractors (ZPIC), Program Safeguard Contractors (PSC), and Common Working File (CWF) host contractors who use the data to investigate fraudulent claims.

Describe the procedures for accounting for disclosures.

FPS direct contractors must sign the Data Use Agreement (DUA) prior to receiving the data in the FPS system. All data is provided to the FPS via reporting and the distribution of each report is tracked. CMS monitors the distribution of the reports and can identify when FPS has received the data and reports.

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 FPS receives PII from other CMS systems, which are responsible for notification to individuals whom the information was collected from.

The FPS system collects information from CMS systems and not individuals directly through DUAs. Information is collected from the following systems who each have a PIA:

Beneficiary Complaints Data CMS Shared Systems Common Working File Enrollment Database (EDB)
Healthcare Integrated General Ledger Accounting System (HIGLAS)

Integrated Data Repository (IDR) Medically Unlikely Edits System (MUE) Medicare Beneficiary Database (MBD) Medicare Exclusion Database (MED) National Claims History (NCH)
National Fraud Investigation Database (FID)

Provider Enrollment Chain and Ownership System (PECOS)

Individuals with usernames and passwords from users that access the system fill out an application for access to the system and they are notified of their rights under the Privacy Act Statement on the application.

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.

The FPS system collects information from other CMS systems and not individuals directly through DUAs. Information is collected from the following systems who each have a PIA:

Beneficiary Complaints Data CMS Shared Systems Common Working File Enrollment Database (EDB)
Healthcare Integrated General Ledger Accounting System (HIGLAS)

Integrated Data Repository (IDR) Medically Unlikely Edits System (MUE) Medicare Beneficiary Database (MBD) Medicare Exclusion Database (MED) National Claims History (NCH)
National Fraud Investigation Database (FID)

Provider Enrollment Chain and Ownership System (PECOS)

There are no opt-out methods for users requiring access to the system because their information is needed for account creation.

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

The FPS system collects information from other CMS systems and not individuals directly. Information is collected from the following systems who each have a PIA:

Beneficiary Complaints Data

CMS Shared Systems

Common Working File

Enrollment Database (EDB)

Healthcare Integrated General Ledger Accounting System (HIGLAS)

Integrated Data Repository (IDR)

Medically Unlikely Edits System (MUE)

Medicare Beneficiary Database (MBD)

Medicare Exclusion Database (MED)

National Claims History (NCH)

National Fraud Investigation Database (FID)

Provider Enrollment Chain and Ownership System (PECOS)

System adminitrators are notified that their PII (user credentials) is being collected per notice on the login page.

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.

Individuals are notified annually in the Medicare & You handbook of their right to file a complaint if they believe their privacy rights have been violated. The 1-800-MEDICARE phone number is included in the handbook and there is more information on www.medicare.gov. When an individual calls 1-800-MEDICARE, the appropriate area at CMS would work with the individual to make sure the complaint is resolved.

Users and administrators who are concerned that their user/admin credentials have been compromised are required to follow the CMS policy regarding Incident Response reporting. Individuals concerned about the accuracy of their records should contact the Director, Program Integrity Group, Office of Financial Management, CMS who will assist in resolving the concern.

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 FPS system adheres to CMS Security and Privacy requirements as set forth by the National Institutes of Standard and Technology 800-53. PII cannot be modified by any individual to include systems administrators who use the system. Policies are in place to detect and protect the system from unauthorized changes based on secure system baseline configurations. Each user must have a unique ID which allows for no repudiation on the system. The system maintains availability in accordance with CMS requirements to ensure that PII is available to investigators as needed for their investigations of fraud. Outdated, unnecessary, irrelevant, incoherent, and inaccurate PII is removed from the system in accordance with CMs requirements for retention of data.

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

Users:

The system will share or disclose data with other CMS direct contractors including Medicare Administrative Contractors (MAC), CMS Enterprise Data Centers (EDC) hosting the CMS claims processing system, Recovery Audit Contractors (RAC), Zone Program Integrity Contractors (ZPIC), Program Safeguard Contractors (PSC), and Common Working File (CWF) host contractors. Such PII can include Name, Email Address, Phone Numbers,
Medical Notes, Date of Birth and HICN/Beneficiary information in order to aid in investigation of fraud, waste and abuse.

Administrators:

System Administrators provide support for the midrange operating system on which the Predictive Modeling System application suites run. They provide support for the database which the Predictive Modeling System application suite uses. Database which the Predictive Modeling System application suite uses. Network Administrators provide support for the firewalls and connections used by the Predictive Modeling System software suite.

Developers:

Developers may have access to PII to include Name, E-Mail Address, Phone Numbers, Medical Notes, Date of Birth and HICN/Beneficiary information in order to develop and fine tune the FPS models to more accurately determine and prevent fraudulent claims through predictive analytics.

Contractors:

Administrators and Developers who consist of direct contractors may have access to PII to include Name, E-Mail Address, Phone Numbers, Medical Notes, Date of Birth and HICN/Beneficiary information in order to develop and fine tune the FPS system to more accurately determine and prevent fraudulent claims.

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

The FPS system adheres to CMS Security and Privacy requirements as set forth by the National Institutes of Standard and Technology. Technical controls such as access controls and identification and authentication are in place to determine which user can access PII. Users must be authorized through FPS System Administrators before they can access any information to include PII. Access is granted based on least privileges policies to ensure authorized access is only the minimum rights needed to perform job functions. Also policies are in place to detect and protect the system from unauthorized changes based on secure system baseline configurations. Each user must have a unique ID which allows for no repudiation on the system.

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 permitted based upon the Need to Know and Least Privilege principles; physical and logical access is governed by CMS Acceptable Risk Safeguards (ARS) version 2.0 and Federal Information Security Management Act (FISMA) requirements. FPS utilizes logical access controls based on job requirements to restrict access to mainframe and network applications. Physical access controls (card readers, ID cards) are used to restrict entry to critical areas to authorized staff. Access is granted based on individual job responsibilities. All access is granted based on management approval.

It is policy that all user access is role/user based. Management approved profiles have been established to limit the transactions that can be processed by a user in a specific role. The only access received by a user is limited to what their job responsibility necessitates. Any attempt to access information outside of approved applications will result in a denial (system generated) and the attempt will be logged. The violation reports will indicate the number of attempts and after a pre-established threshold is met, the violation is investigated.

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.

The security awareness program includes Security Training for new workforce members, and annual refresher security awareness training for current workforce members and other activities that promote security awareness throughout the organization

All employees receive basic information security awareness training prior to being allowed access to any Information System, when required by system changes and annually thereafter.

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

All users are required to complete Security Awareness training prior to accessing systems. This training includes information on security expectations required of users, password management and the Rules of Behavior. Newly hired workforce members must sign an attestation that they have completed the training and have read and understand the Rules of Behavior once the training has been completed.

Annual refresher training and occasional management modules on security are also used to disseminate information on security. Fire drills are also conducted at least annually.

Personnel with significant information security roles and responsibilities (employees and direct contractors) will undergo information system security training prior to authorizing access to CMS networks, systems, and/or applications; when required by system changes; and refresher training annually thereafter. All employees undergo security awareness training. Additionally, those employees that have CMS Public Health Information (PHI) access undergo Health Insurance Portability and Accountability Act (HIPAA) training.

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 Schedules (RSC) # N1-440-09-015: DISPOSITION: TEMPORARY Cut off at the end of the Fiscal Year 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.

Access to the system is given based on need to know and job responsibilities. The Fraud Prevention system is processed in an approved CMS data center. FPS uses security software and procedural methods to provide "least privilege access" to grant or deny access to data based upon need to know. External audits also verify these controls are in place and functioning.

Administrative Controls are in place for FPS2 to include security training and awareness. All users are required to complete security awareness training and sign Rules of behavior acknowledging safeguarding PII. Disaster preparedness and recovery plans are in place to ensure users are prepared in the case of emergency and incident response training is also administered to ensure proper reporting and handling of suspected or known incidents involving PII.

Technical controls include user identification, passwords, firewalls, virtual private networks and intrusion detection systems.

Physical controls used real-time alarms generated by the access control system. All devices are networked, so if there is an issue, the access device will get an alarm work order and send to support services. All doors are alarmed for 'forced-open' and anytime a door is held opened. The control room can generate a screen shot, or produce an alarm report to reflect whether a door was forced or held open.