US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/06/2026

OPDIV:

CMS

Name:

Provider Enrollment Chain and Ownership System

PIA Unique Identifier:

P-3749030-384886

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?

Yes

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.

PECOS scheduled quarterly releases in accordance with change management and CMS Acceptable Risk Safeguards.

Describe the purpose of the system.

The Provider Enrollment Chain and Ownership System (PECOS) serve as a national database of Medicare Provider information. The database contains information related to ownership, managing employees, billing arrangements, re-assignment of benefits, practice locations, and related organizations for Medicare providers.

Core Functions:

The primary function of PECOS is the capture and management of enrollment information.

PECOS allows enrollment of Medicare providers – both individuals and institutions

Collects, relates, and stores Medicare provider enrollment information in a national database.

Allows organizations and individuals to initiate the Medicare enrollment process or make update to an existing enrollment via a web- or paper-based application. The enrollment information is electronically stored and shared with other systems. The data is collected to enable providers to bill to Medicare, and to also assist with CMS fraud prevention.

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

Provider information is collected and stored such as: Name, Date of Birth (DOB), Mailing Address, Financial Account Information, Employer Identification Number (EIN), Taxpayer ID, Social Security Numbers (SSN), Driver's license Number, Email Address, maiden name, phone numbers, certificates, vehicle and photographic identifiers, medical notes, and educational records. User credentials, such as user ID, are captured for auditing purposes only.

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

The Medicare Federal Health Care Provider/Supplier Enrollment Application (CMS 855A, 855B, 855I, 855O, and 855S) has been designed by the Centers for Medicare and Medicaid Services (CMS) to assist in the administration of the Medicare program and to ensure that the Medicare program follows all regulatory requirements. Provider information collected in this application, including name, application User ID, DOB, EIN, Taxpayer ID and SSN if applicable, will be used to ensure that payments made by the Medicare trust fund are only paid to qualified health care providers, and that the amounts of the payments are correct.

This information will also identify whether the provider is qualified to render health care services and/or furnish supplies to Medicare beneficiaries. To accomplish this, Medicare must know basic identifying and qualifying information about the health care provider that is seeking billing privileges in the Medicare program. Medicare needs to know: (1) the type of health care provider enrolling, (2) what qualifies this provider as a health care related provider of services and/or supplies, (3) where this provider intends to render these services and/or furnish supplies, and (4) those persons or entities with an ownership interest, or managerial control, as defined in this application, over the provider. The data includes PII information from providers.

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
Photographic Identifiers
Driver's License Number
Mother's Maiden Name
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Medical Notes
Financial Accounts Info
Certificates
Education Records
Taxpayer ID
Application User ID, Maiden Name, Employer Identification Number (EIN)

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

Public Citizens
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

Fiscal Intermediary Standard System (FISS), Multi-Carrier System (MCS) and ViPS Medicare System (VMS) claims payment systems – to populate the claims system provider files.
National Plan & Provider Enumeration System (NPPES) – to verify National Provider Identifier (NPIs).
Social Security Administration (SSA) – to verify SSNs.
Medicare contractors, CMS Central Office, CMS Regional Office to research or verify provider/supplier enrollment data.
FISS, MCS, VMS and NPPES are covered under their own PIAs.

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.

(CMS) is authorized to collect the information requested on 855 forms by sections 1124(a)(1), 1124A (a)(3), 1128, 1814, 1815, 1833(e), and 1842(r) of the Social Security Act [42 U.S.C. §§ 1320a-3(a)(1), 1320a-7, 1395f, 1395g, 1395(l)(e), and 1395u(r)] and section 31001(1) of the Debt Collection Improvement Act [31 U.S.C. § 7701(c)].

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.

09-70-0532 (PECOS)

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Hardcopy
Online
Government Sources
Other Federal Entities
Non-Governmental Sources
Public
Private Sector

Identify the OMB information collection approval number and expiration date

The PECOS OMB control numbers and associated expiration dates are outlined below:

- 0938-0685 (CMS-855A): 9/30/2027
- 0938-1377 (CMS-855B): 12/31/2028
- 0938-1355 (CMS-855I): 5/31/2026
- 0938-1135 (CMS-855O): 5/31/2026
- 0938-1056 (CMS-855S): 2/28/2026

The OMB control number for 0938-1056 is pending OMB approval to be reinstated.

Is the PII shared with other organizations?

Yes

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

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

Privacy act for System of records. Computer Matching and Privacy Protection Act of 1988 (P. L. 100-503) amended the Privacy Act, 5 U.S.C. § 552a, to permit the government to verify information through computer matching.

There is a Memorandum of Understanding (MOU) in place between CDS and CGI Federal.

Describe the procedures for accounting for disclosures.

PECOS follows all CMS policies and procedures for accounting disclosures of information. Procedures for accounting for disclosures must be requested and logged by the PECOS ticket tracking system. The ticket author is a surrogate of the actual requestor, because the requestor will not have access to the PECOS internal ticket tracking system. The procedure is managed in the agreements in place with other Private Sector, Federal agencies and State 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.

Instructions on 855 Forms notify the individuals that personal information is required to process the Enrollment application. All information collection changes are submitted to OMB for agency and public review & comment and for OMB approval prior to implementation.

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 information will be collected from all health care providers and suppliers who render services or supplies to Medicare beneficiaries and bill the Medicare program for those services and supplies. This information will be collected via the completion of the CMS 855, Provider/Supplier Enrollment Application. All this information is conveyed to the providers of the information in writing directly on CMS 855 and on the certification signature page of the form.

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

The CMS form 855 has a Privacy Act Statement which gives the purpose of the information. Also, any changes to the enrollment application do not alter the PII information unless initiated by the Individual. In the event of any changes, users are notified of the changes via website notice.

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.

Providers can call their Medicare Contractor or CMS Contracting Officer (CO) or Contracting Officer Representative (COR) to resolve any issues or concerns related to PII.

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

Part A/B Providers and suppliers are required to revalidate their information every 5 years and Durable Medical Equipment (DME) suppliers every 3 years. During the revalidation process and for any change of information submitted by the Providers, the PII data is validated against NPPES and SSA.

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

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

Those with access to PII have only the minimum access necessary to perform their job function in accordance with the least privilege principle.

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.

Role based access is implemented, each user can only access PII data that is granted to their role.

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 CMS employees and contractors with access to CMS networks, applications, or data must complete mandatory annual Security and Privacy Awareness Training, also known as Computer-Based Training (CBT) annually. This training must be completed initially when a user first receives their CMS Enterprise User Administration (EUA) account and annually thereafter as part of the annual re-certification process.

Additionally, users logging into the application for the first time must acknowledge a Rules of Behavior agreement before proceeding; content is in-line with standard CMS training.

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

CMS employees and contractors with privileged access are required to complete role-based training and meet continuing education requirements commensurate with their role and participate in an annual contingency planning exercise. Additionally, contractors also complete corporate information security training prior to being assigned to a project and repeat annually.

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.

There is a 7-year retention policy for enrollment information. Any records that are needed longer, such as audit or other exceptions, will be retained until such matters are resolved by National Archives Record Association (NARA) Records Schedule Number N1-440-09-018.

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

PII is secured in the system using administrative, technical, and physical controls, in accordance with policies and regulations detailed in the CMS Acceptable Risk Safeguards (ARS) standards.

[Administrative] Administrative controls include security awareness training, organizational security policies and procedures, and background checks for organizational users.

[Technical] Technical controls include role-based access control, multifactor authentication, firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), etc. to prevent unauthorized access to the system.

[Physical] PECOS is hosted in a data center and will be protected through intrusion alarm, surveillance equipment, and biometric/badge readers.

Identify the publicly-available URL:

URL: https://Pecos.cms.hhs.gov

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

No

Does the website use web measurement and customization technology?

No

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

No