US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/22/2016

OPDIV:

CMS

Name:

National Plan and Provider Enumeration System

PIA Unique Identifier:
P-4465596-228950

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.
Identity and Access (I&A) module has been enhanced.

Describe the purpose of the system.
The National Plan and Provider Enumeration System (NPPES) serves as the national system designed to assign unique identifiers to health care providers and health plans who apply for the National Provider Identifier (NPI). NPIs are being used across the health care industry and government health care programs. Computer systems that serve providers, health care plans, Medicare and Medicaid are the target users of these NPIs. NPPES contains information that is used to uniquely identify the health care provider and health plan.

Describe the type of information the system will collect, maintain (store), or share.
NPPES: The system contains a unique identifier for each health care provider (the NPI, which is assigned by the NPPES) along with other information about the provider including:

Provider Name, Gender, Social Security Number (SSN), Tax Identification Number(TIN), Individual Tax Payer Identification Number(ITIN), Date of Birth (DOB),Place of Birth, Address and Phone numbers, professional and commercial data.Additionally, demographics like race and ethnicity may be stored as optional fields.

Identity & Access (I&A): The system contains account information along with other information about the external user. The users of the NPI system include Providers, Enumerators, CMS Staff, and the healthcare Industry. Information includes name, Date of Birth (DOB), Social Security Number (SSN), phone number, employer information, and relationships to provider organization(s) and individual provider(s) in NPPES. The I&A system is a module within the NPPES security boundary. Users are required to get an I&A account to access the NPPES system. The NPPES system also obtains updated Provider/User information from CMS' Provider Enrollment Chain and Ownership System (PECOS). They share an application program interface (API) with PECOS that is within the CMS boundary. PECOS has 'Write' privileges to provide updated information through the API and this information later gets stored in the NPPES database.

NPPES also stores internal user log in credentials and passwords for authentication purposes. The log in credentials comprise the User ID and Password and the users are System Administrators (CMS employees and direct contractors).

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

The Centers for Medicare and Medicaid Services (CMS) has developed the National Plan and Provider Enumeration System (NPPES) that provides unique National Provider Identifiers (NPIs) for health care providers and health plans. NPIs are expected to be used across the health care industry and government health care programs; Computer systems that serve providers, health care plans, Medicare and Medicaid are the target users of these NPIs. NPPES has a Public Search page that can use Non-PII information as search criteria in order to stream- line their search.
The users of the NPI system include Providers, Enumerators, CMS Staff, and the healthcare Industry.

NPPES permanently stores PII and non-PII to identify individual and organizational Providers. NPPES enumerates providers by assigning them an NPI. The NPPES system collects and stores the following Provider information: Provider Name, Gender, Social Security Number(SSN), Tax Identification Number(TIN), Individual Tax Payer Identification Number(ITIN), Date of Birth (DOB), Place of Birth, Address and Phone numbers, professional and commercial data. Users have the ability to update their PII after proper authentication and validation to access their accounts in the NPPES system.

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

E-Mail Address

Mailing Address

Phone Numbers

Employment Status

Passport Number

Taxpayer ID

Other: User/System Admin credentials- User ID and password; TIN; ITIN; race; ethnicity; gender

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

Employees

Public Citizens

Other: Public citizens who are health care providers

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The purpose is to collect the information needed to uniquely identify an individual health care provider, to assign an NPI to that health care provider, to maintain and update the information about the health care provider, and to disseminate health care provider information in accordance with the provisions of the Privacy Act.

The primary purpose for the collection of the user/system administrator credentials is for authentication of the system users to prevent unauthorized access of the system.

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

PII may be shared with other agency systems, to ensure data consistency and accuracy.

Describe the function of the SSN.

To assist in accurately identifying providers and avoid duplication of providers/records.

Cite the legal authority to use the SSN.

Database checks required by CMS Rule 6028 FC and 42 CFR §424.518, including screening against Social Security Number (SSN), the National Provider Identifier (NPI), the National Practitioner Data Bank (NPDB) licensure, an OIG exclusion; taxpayer identification number; tax delinquency; and the death of individual practitioner, owner, authorized official, delegated official, or supervising physician. The direct contractor shall also check individuals for felony convictions. In order to complete these checks, CMS will provide access to the NPPES, National Provider Database (NPDB), Medicare Exclusion Database (MED), Fraud Investigation Database(FID), and Compromised Number Checklist (CNC). The SSN is used in conjunction with the other PII as a confirmation that the PII is correctly linked to a specific provider.

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

Database checks required by CMS Rule 6028 FC and 42 CFR §424.518, including screening against Social Security Number (SSN), the National Provider Identifier (NPI), the National Practitioner Data Bank (NPDB) licensure, an OIG exclusion; taxpayer identification number; tax delinquency; and the death of individual practitioner, owner, authorized official, delegated official, or supervising physician. The Direct Contractor shall also check individuals for felony convictions. In order to complete these checks, CMS will provide access to the NPPES, NPDB, MED, FID, and CNC.

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.

National Provider System (NPS), No. 09-70-0008

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Online

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

OMB approval number: 0938-0931
Expiration Date: 4/30/2018-currently in process for updated approval.

Is the PII shared with other organizations?

Yes

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

Within HHS

Within HHS we share Provider Information to PECOS to automatically update Provider data.

Other Federal Agencies

Information is disclosed to Department of Justice, Office of Inspector General to conduct ongoing investigation, and to the Federal Bureau of Investigation (FBI) (only on request) to conduct any ongoing investigations.

State or Local Agencies

Information is disclosed to state agencies to allow for identifying enumerated providers to validate information and conduct ongoing investigations.

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

Data Use Agreements (DUA) are in place whenever PII is shared. The associated documentation describes the type of information to be shared as well as the conditions under which it will be shared, with whom it will be shared and the business justification that documents why the information is shared.

Describe the procedures for accounting for disclosures.

For approved disclosures, PII tracking elements are in place and follow the process defined in the DUA. PII is available for public search on the NPPES NPI Registry site. Examples of disclosed PII are name, phone number, and address. DUAs track the PII that is disclosed, when it is disclosed, who it is disclosed to, and for what purpose.

https://npiregistry.cms.hhs.gov/registry/provider-view/1710397443

This process accounts for the date, nature, and purpose of each disclosure and the name and address of the recipient.

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 Privacy Act statement listed on the website provides notifications to individuals of the provisions for individuals to provide consent for a data collection. The submission of the data is mandatory for an individual provider to participate in the Medicare program.

If an individual wants to inquire if their PII is included in this CMS information system, they should write the system manager listed on this document, who will require the system name, provider name, and, for verification purposes, date of birth, and medical school (if applicable), to ascertain whether or not the individual's record is in the system.

During invalid log in attempts the user receives a message that the user ID or password is incorrect. This message is indicative of the fact that the system stores user/administrative log in and passwords for authentication purposes.

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.

NPPES: Information collected via the NPPES web site (internet) or paper application. Notification of NPI given via e-mail (if application was via web) or paper letter if application was via paper. Information is provided on the paper form and on the web screens regarding the Certification Statement and the Privacy Act Statement.

I&A: Information is collected via the I&A web site (internet). Notification is given via e-mail. Access to I&A is provided through systems that contain Certification Statements and the Privacy Act Statement (such as PECOS and EHR IP).

Since the system also stores user Log in credentials and passwords, there is no opt-out for this information collection.

The information disclosed on the NPI Registry and in the downloadable files are Freedom of Information Act (FOIA)-disclosable and are required to be disclosed under the FOIA and the eFOIA amendments to the FOIA. There is no way to 'opt out' or 'suppress' the NPPES record data for health care providers with active NPIs.

Reference:
https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/NationalProvIdentStand/DataDissemination.html

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

PII is required for assigning an NPI. Consent is not required from individuals whose PII is already in the system, when major changes occur to the system and /or the purpose and disclosure of data changes from its original purpose and disclosure. The reason for not asking for user consent is because the data is already within the security boundaries of CMS and all system changes are approved by the Business owner. System Notifications will be posted of any major enhancements to the system.

The same holds true for user/system administrator credentials and passwords that are stored by the system for authentication purposes.

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 should contact the CMS IT Service Desk at 410-786-2580 to submit an incident request if they believe their PII has been inappropriately obtained, used, or disclosed. This is accordance with the CMS Breach Notification Procedures.

The system also stores user log in credentials and passwords for authentication purposes. If users forget their credentials or password, they can contact the IT help desk to resolve their issue.

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

If it is believed that a HIPAA-covered entity or its business associate violated an individual's (or someone else’s) health information privacy rights or committed another violation of the Privacy, Security, or Breach Notification Rules, the individual may file a complaint with the Office for Civil Rights (OCR). OCR can investigate complaints against covered entities (health plans, health care clearinghouses, or health care providers that conduct certain transactions electronically) and their business associates.

Anyone can file a health information privacy or security complaint. The complaint must:

Be filed in writing by mail, fax, e-mail, or via the OCR Complaint Portal Name the covered entity or business associate involved, and describe the acts or omissions, you believed violated the requirements of the Privacy, Security, or Breach Notification Rules be filed within 180 days of when you knew that the act or omission complained of occurred. OCR may extend the 180-day period if you can show "good cause".

Furthermore, the individual can contact the system manager named in this document to dispute any inaccuracy of the PII in the system, and reasonably identify the record and specify the information to be contested. State the corrective action sought and the reasons for the correction with supporting justification.

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

Providers are asked to verify/certify that the data they entered in the NPPES system is accurate before submission. Users are able to view their records, and can edit some fields or request other fields to be updated as appropriate. PII fields can be updated when required through the individual user accounts that are created in the NPPES system. Access to these accounts is provided after proper authentication of the user. PII is stored in the individual accounts which also include user log in credentials and passwords for authentication purposes.

In addition, when Providers update their information in the Provider, Enrollment, Chain and Ownership System (PECOS), the PECOS system can update the NPPES system with the new information through an API system that resides within the security boundaries of CMS. This process helps in the storage of accurate and updated data.

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

Users:

Users need access to the PII in the system to verify the accuracy of their information. If they need to update the data they can do so with the interventions of CMS and verification.

User credentials and passwords that are stored in the system can be changed by contacting the CMS IT Help Desk or via NPPES web application.

Administrators:

Administrators need to access to PII for Data correction, maintenance, problem resolution.

Administrators monitor the changes in the user credentials and passwords, as they are stored by the system.

Developers:

Developers need to access PII for Problem resolution and testing purposes

Contractors:

Direct contractors need access to PII for Data entry and validation. Validation of the user/admin credentials is also done as the system also stores user Log in credentials and passwords for authentication/Validation purposes

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

The system applies role based access in system for users to ensure that users are only provided access to PII data that is required to complete their duties. Only system administrators will be able to assign roles to users based on their need-to-know. Enumerator staff will have access to the User Profile to assist the Users when they have any issues. End User Service (EUS) staff will have access to the User Profile to assist the Users when they have any issues.

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.

The following controls limit a user’s access to the type, amount, or categories of PII necessary to perform their job functions:

AC-5 Separation of duties: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion.
AC-6 Least privilege: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions.
AC-6(5): The organization restricts privileged accounts on the information system to defined personnel or roles (defined in the applicable security plan). The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions.

AC-6(10) Prohibit Non-Privileged Users from Executing Privileged Functions. Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations.

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 are users of the system are required to take annual CMS Information Security and Privacy Awareness Training for protecting the information being collected and maintained.

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

Not applicable

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.

System records are housed in both active and archival files in accordance with CMS data and document management policies and standards including GRS 3.2.

National Archives and Records Administration (NARA), General Records Schedule (GRS) 3.2 states that CPMS will destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the Certification Authority, or when no longer needed for business, whichever is later. The records in the NPPES system are retained indefinitely, except in the instance of an individual provider's death, in which case CMS would retain such records for a minimum of a 10-year period following the provider's death.

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

NPPES secures PII by implementing a multi-tiered architecture using multiple types and layers of firewall and intrusion detection technology.

Administrative controls: Access to the data is granted on a 'need to know' basis. External audits are used to verify/validate all implemented controls. CMS Standards are followed for software and hardware, as well as data protection and maintenance.

Technical controls: user identification, passwords, security tokens, firewalls, virtual private networks and intrusion detection systems.

Physical controls: guards, identification badges, key cards, cipher locks and closed circuit televisions.

Identify the publicly-available URL:

NPPES : https://nppes.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?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

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

No

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

No

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

null