US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/16/2016

OPDIV:

CMS

Name:

Internet Services

PIA Unique Identifier:

P-5162391-134893

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.

No changes have occurred.

Describe the purpose of the system.

Internet Services is a collection of automated systems that directly provides the public with healthcare consumer information (e.g., CMS program eligibility and coverage, provider availability and quality, claim status). These systems make up the CMS e-Government presence and are the official public Agency websites for the Centers for Medicare & Medicaid Services. The systems covered under Internet Services include the following websites:
Medicare.gov (www.medicare.gov)
Plancompare.medicare.gov (plancompare.medicare.gov)
Online Enrollment Center (enrollmentcenter.medicare.gov)
CMS.gov (www.cms.gov)
Medicaid.gov (www.medicaid.gov)

CMS Innovation Center (innovation.cms.gov)
InsureKidsNow.gov (www.insurekidsnow.gov)
Partnership for Patients (partnershipforpatients.cms.gov)
Downloads.cms.gov (downloads.cms.gov)
Data Navigator (dnav.cms.gov)
Stop Medicare Fraud (www.stopmedicarefraud.gov)
The first 4 sites listed contain dynamic applications and are only available via HTTPS. The remaining sites contain only static content, but may also force HTTPS.

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

The following is a list of all types of information that Internet Services (IServ) collects in order to retrieve filtered results from read-only databases, across the various applications hosted on the IServ sites. Note that these inputs are not stored by the application; they are only used to filter the datasets:
Search Location (ZIP Code, City/State, State);
Specialty (e.g. Cardiology);
Organ or organ system (e.g. Heart);
Last name of a healthcare professional;
Group practice name;
Hospital name;
Medicare assignment status of healthcare professional;
Nursing home name;
Home health name;
Dialysis facility name;
Supplier product category;
Publication category;
Publication language preference;
Publication keyword;

The following list of inputs are collected and stored by the Online Enrollment Center in order to provide application details to the health/drug plan:
Selected Plan Details;
Prescription Drugs Used (optional);
Preferred Pharmacies (optional);
Reason for Enrollment Eligibility;
Title (Mr., Mrs., Miss., Ms.);
Full Name;
Date of Birth;
Gender;
Email Address (optional);
Home Phone Number;
Permanent Residence;
Mailing Address;
Emergency Contact (optional);
Medicare Claim Number;
Medicare Claim Number Effective Date (Part A);
Medicare Claim Number Effective Date (Part B);
Premium Payment Method;
Additional Drug Coverage Plan Details (if applicable);
Long-Term Care Facility Details (if applicable); Health Insurance Claim Number;

The following list of inputs are collected and stored by the Ordering application in order to ship printed booklets to the user:

Full Name;
Shipping Address;
Phone Number (optional);
Email Address (optional);

PII collected from users/system administrators in order to access the system, consists of user credentials (i.e. username, password, Personal Identity Verification (PIV) card and/or email address). Users/system administrators include CMS employees and direct contractors (using HHS user credentials only).

Note: Additional details regarding the Privacy Impact Analysis (PIA) for Third-Party Websites and Applications (TPWA) used by CMS can be found at www.hhs.gov/pia/index.html#Third-Party.

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

Internet Services is a collection of automated systems that directly provides the public with healthcare consumer information (e.g., CMS program eligibility and coverage, provider availability and quality, claim status). These systems make up the CMS e-Government presence.

The majority of the dynamic applications only request basic information like location to search (e.g. ZIP code or city/state) and some application-specific search criteria (e.g. a physician's specialty, like cardiology). These search criteria are only maintained for the duration of the user's browser session and are then discarded. This search criteria is used to provide results that match the user's requested filters (ex ZIP Code, Physician's specialty, etc). In most cases, these filtered results are pulled from publicly available datasets. The following items are exceptions, where user entered data is stored by one of the Internet Services applications: When required data elements such as first name, last name and address are collected from the users of Medicare.gov. during Publications Ordering; When ZIP code, Health Insurance Claim Number (HICN), Last Name, Medicare Effective Date, and Date Of Birth (DOB) information is sought by the Medicare Plan Finder tool to help retrieve additional beneficiary information, including details regarding the plan user is currently enrolled in. This information is self-entered by the user and only used for the duration of their web browser session; When a stream-lined version of this tool is used by Customer Service Representatives (CSRs) in the 1-800-Medicare call centers to help authenticate the user and provide personalized drug plan information.

Data is collected to: improve the Agency's web site; allow visitors to ask specific questions of Agency staff, and support conference registrations for outreach and educational purposes. At all data collection points, a link to the web site privacy policy is provided (the privacy policy is linked from the web site footer so that it is available on all pages). When a user submits feedback they get a response explaining how their data will be used. Similarly, conference registrants receive an email confirmation explaining the use of their data. Information is collected at several points in the site.

Specifically, users can submit feedback and questions through our "Feedback" link. The only data element explicitly requested is an email address. This is a voluntary submission. These feedback requests are triaged automatically to the appropriate business component for response. Additionally, we have an online conference registration system available. This system captures contact information from registrants, including, name, business, address, phone, fax, and email. This information submission is voluntary and is automatically sent to the conference coordinator and removed from the web site after 60 days.

Information is collected from users of Online Enrollment Center during the enrollment process and the required data elements include: Name, Address, Phone Number, E-mail Address, Health Insurance Claim Number (HICN), Date of Birth, and monthly premium withhold preference.

Other information collected from users are of a voluntary nature, such as Mailing Address and emergency contacts. Information is used to enroll users in Part C or Part D programs. Collection of required information is necessary so that plan sponsors can validate personal information of users enrolling in their plan as well as to validate user's eligibility status with CMS and the Social Security Administration. CMS employees and direct contractors provide their login credentials for local/administrator access to back-end systems.

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

Financial Accounts Info

Other: Health Insurance Claim Number (HICN), Organization Name, user credentials: user ID and HICN

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

Employees

Public Citizens

Patients

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

Medicare Plan Finder has a general search option. However, if users would like personalized search results with details specific to their situation, they can provide ZIP code, Health Insurance Claim Number (HICN), Last Name, Medicare Effective Date, and Date Of Birth (DOB). This information is self-entered by the user and only used for the duration of their web browser session.

The Medicare.gov site provides users with the ability to order printed versions of Publications. The Ordering workflow requires the user to enter First Name, Last Name, and Mailing Address in order to mail them the printed version. Optionally, the user can also provide their Phone Number or E-mail Address.

The Online Enrollment Center allows users to enroll in a Medicare plan. In order to enroll in a plan, the user must provide the following information to the plan sponsor, so they can verify the user's eligibility: Name, Date Of Birth (DOB), Gender, Phone Number, Mailing Address, Health Insurance Claim Number (HICN), Medicare Effective Dates, and Other Insurance Coverage.

Login credentials for local access/administrator to backend systems (all the servers that comprise the system) are stored on the backend systems. They include a username consisting of a randomly generated character alpha-numeric string, and a password.

In all cases, the Internet Services Privacy Policy is available to view from the footer of the websites.

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

Not Applicable

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

Authority for maintenance of the system is given under sections 1102, 1804(b), and 1851(d) of the Social Security Act (42 United States Code (U.S.C.) 1302, 1395b–2(b), and 1395w– 21(d)), 5 USC 301, Departmental Regulations, and Title 42 U.S.C. section 1395w–21 (d) (Pub. L. 105–3, the Balanced Budget Act of 1997).

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.

1–800 Medicare Helpline (HELPLINE), System No. 09–70–0535

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

OMB Number: 0938-0951
Expiration Date: 2/28/2017

Is the PII shared with other organizations?

No

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

There is no prior notice given to inform individuals that their personal information will be collected because the Internet Services Privacy Policy is available to view from the footer of all pages on the websites and states within it:

CMS websites don't collect any Personally Identifiable Information (PII) about individuals during their visit unless they choose to provide it to us.

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 user has the option to perform a General search instead and the following text is provided to guide the user in their choice: “If you don’t want to enter your Medicare information, you may use the general search option above.”

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

Individuals submit PII for the purpose of obtaining search results from Medicare Plan Finder, Medicare.gov and Online Enrollment Center. If CMS makes a major change related to the system, CMS will update online notices on CMS.gov (www.cms.gov/About-CMS/Agency-Information/Aboutwebsite/Privacy-Policy.html).

This privacy policy covers all sites within Internet Services.

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.

If a user believes their PII has been inappropriately obtained, used, or disclosed: They should first contact the 1-800-MEDICARE Call Center. The Medicare Call Center will then report the issue to the Office of Communications (OC) / Web and New Media Group (WNMG) and the CMS Privacy Office who will investigate the incident. WNMG will work with its resources and the Privacy Office to determine the root cause of the issue, resolve the immediate issue, and put in additional safeguards to ensure that the issue does not occur again.

If a user believes their PII is inaccurate: They should first contact the 1-800-MEDICARE Call Center. The Medicare Call Center may be able to address the inaccurate PII, depending on exactly where the data is stored. If the Medicare Call Center is unable to resolve the inaccurate PII date issue on their own, they will then report the issue to the Office of Communications (OC) / Web and New Media Group (WNMG). WNMG will work with the individual to have their data corrected.

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

CMS has a National Institute of Standards and Technology (NIST) compliant continuous monitoring program to ensure system integrity and availability.

IServ has firewalls and databases that are not directly exposed to ensure integrity. Iserv is in a world-class data center and has a redundant server farm to ensure availability.

With respect to accuracy and relevancy of PII, it is submitted and managed by the user. For the Online Enrollment Center (OEC) and Ordering workflows where users submit PII that is stored in the system, this is a one-way, one-time insert. If a user needs to correct his/her information, he/she will need to resubmit his/her request.

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

Administrators:

To ensure data Confidentiality, Integrity and Availability.

Developers:

Our contracted developers have administrative rights in order to complete their system development and operation tasks.

Contractors:

Our direct contracted developers have administrative rights in order to complete their system development and operation tasks.

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

CMS uses role-based access controls to ensure administrators and direct contractors are granted access on a "need-to-know" and "need-to-access" commensurate with their assigned duties. The business owner of the system grants access.

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.

There are three methods for restricting access. First, is to program user interfaces to limit the display of PII to only those elements needed to perform specific tasks. Second, is to limit the transmission of PII to validate information rather than copy or pull information form another authoritative source. Third, is to implement role based access controls and auditing to ensure those with access have a "need-to-know" and "need to access".

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.

Both Federal and CMS Direct Contractor staff who access or operate a CMS system are required to complete the annual CMS Security Awareness training provided annually as a Computer Based Training (CBT) course. Contractors also complete their annual corporate security training.

Individuals with privileged access must also complete role-based security training commensurate with the position they are working in.

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.

IServ follows the CMS Records Schedule, which is aligned with the National Archives Records Administration (NARA) Records Control Schedule DAA-GRS-2013-0006-0003- Destroy 1 year(s) after user account is terminated or password is altered or when no longer needed for investigative or security purposes, whichever is appropriate; and Disposition Authority: DAA-0440-2012-0005-0013- Cutoff annually. Destroy 7 years after cutoff. In addition, IServ follows the Data Destruction Standards prescribed in NIST Special Publication (SP) 800-88.

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

Administrative – IServ follows the least privilege principle, meaning that only those that require access to the data to perform their duties are actually granted that access. In addition, all CMS employees and contractors are required to take privacy and security awareness training that explains the requirements for handling sensitive data. All security controls are reviewed both internally and by an auditor from a third-party accredited organization (3PAO) during Security Control Assessments (SCA) to ensure compliance with CMS security standards.

Technical - The IServ system is built using industry best practices and independently reviewed against Federal Information Security Management Act (FISMA) and NIST Security and Privacy controls to ensure technical, operational, and management controls are properly applied. This includes the necessary Federal Information Processing Standard (FIPS) 140-2 encryption standards to protect the PII both in transit and at rest. In addition, IServ uses the following security principles: define-in-depth, continuous monitoring, and role-based access control.

Physical - This system is located in a world-class Tier-1 network data center which provides premier physical control protections. The data center undergoes its own Security Control Assessment (SCA) from a 3PAO to ensure compliance with all physical security controls. IServ is managed by Hewlett Packard Enterprise (HPE) Virtual Data Center (VDC). The physical controls that are in place include security guards, video monitoring and the use of security cards for access.

Identify the publicly-available URL:

www.Medicare.gov

www.CMS.gov

www.Plancompare.medicare.gov/Enrollmentcenter.medicare.gov

(User will be redirected to this URL after they select "Plan Compare" option from Medicare.gov link)

www.stopmedicarefraud.gov

www.insurekidsnow.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.

Persistent 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