US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/22/2016

OPDIV:

CMS

Name:

GovDelivery

PIA Unique Identifier:

P-1355245-610860

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?

New

Does the system have Security Authorization (SA)?

Yes

Describe the purpose of the system.

GovDelivery is used to handle email subscription management, and deliver opt-in email. It is designed to facilitate and increase citizen engagement with public government messaging. In another words, it enables citizens (hereinafter referred to as “members of the public”) to more effectively communicate with the Government (hereinafter referred to as “administrators”).

CMS uses GovDelivery to assist with implementing provisions of the Affordable Care Act, to handle outbound communications within the Healthcare.gov ecosystem, and to continually improve communications and access to Agency information on sites Medicare.gov, CMS.gov,Medicaid.gov and Healthcare.gov and CuidadoDeSalud. Gov

It allows subscribers to receive updates when new information becomes available on the CMS websites and automates the creation and distribution of messages through email, text messaging and social media.

GovDelivery sends large volume personalized messages to targeted audiences and provides CMS vital statistics on email delivery rates, open rates and click-through rates used by Healthcare.gov and CuidadoDeSalud.go v (e.g. signup confirmation, password changes, profile changes, etc.).

It manages internal and external questions/requests submitted through the CMS websites and allows end users to submit questions/requests and review the status at any time through Questions.cms. gov, Questions.Med icaid.gov, and Questions.Medicare.gov.

Lastly, it supports collaborative efforts between internal and external stakeholder groups to create project teams and leverage discussion forums to increase staff engagement and share documents and information on projects using Collabgroup.CMS.gov and hfppcomm unity.cms.gov.

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

GovDelivery collects names, telephone numbers, and email addresses of email subscribers.

GovDelivery also manages internal andexternalquestions/requests submitted through theCMSwebsites and allows end users tosubmitquestions/requests and review the status atany time throughQuestions.cms.gov,Questions.Medicaid.gov,and Questions.Medicare.gov.

In addition, GovDelivery supports collaborative effortsbetweeninternal and external stakeholder groupstocreate project teams and leverage discussion forums to increase staff engagement and share documents and information on projectsusing Collabgroup.CMS.gov and hfpp community. cms.gov.

CMS employees and direct contractors support enter user IDs and passwords in order to be granted access to GovDelivery.

Subscribers are also required to enter email addresses and passwords in order to be granted access to GovDelivery.

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

GovDelivery is used to handle email subscription management, and deliver opt-in email. It is designed to facilitate and increase citizen engagement with public government messaging. In another words, it enables members of the public to more effectively communicate with the Government.

The system collects names, telephone numbers, and email addresses. The information is retained until the subscribers cancel his or her subscription. The information collected allows subscribersto receive updates when new information becomes available on the CMS websites, and automates the creation and distribution of messages through email, text messaging and social media. The information collected also allows large volume of personalized messages to be sent to targeted audiences and provide CMS vital statistics on mail delivery rates, and open rates. In addition, the information collected provides a way to manage internal and external questions/requests submitted through the CMS websites and allow subscribers to submit questions/requests and review the status at any time.

CMS employees and direct contractors support enter user IDs and passwords in order to be granted access to GovDelivery.

Subscribers are also required to enter email addresses and passwords in order to be granted access to GovDelivery.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

E-Mail Address

Phone Numbers

Other: User ID and password

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

Employees

Public Citizens

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The PII is purely used for communicating information from CMS about systems and services available to the end user/subscribers.

CMS employees and direct contractor support PII (user IDs and passwords) are used to grant access to GovDelivery and maintain 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.

42 CFR 401.101–401.148

Sec 1106(a) of the Social Security Act,

42 U.S.C. 1306(a)

5 USC 301, Departmental Regulations

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.

Health Insurance Exchanges Program, 09-70-0560

Correspondence Tracking Management System, 09-70-3005

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

N/A: Office of Communication (OC) verified with Office of Strategic Operation and Regulation Affairs (OSORA) that OMB information collection approval is not required as the site does not appear to request or require anything other than contact information for identification purposes. No OMB Control Number applies.

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.

Subscribers are given a signup page, so they know that their personal information is being collected because they entered the information themselves. Additionally, there is a Legal & Privacy statement of the website that describes how GovDelivery will use the information the subscribers provide.

Employees and direct contractors requesting access to GovDelivery must sign an Account request form prior to account creation. Account request form must also be filled indicating name, email, phone number and access level needed. This form is reviewed and approved by the System information Security Officer (ISSO) prior to account creation.

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.

Subscribersare not required to provide PII if they do not want the service. If the CMS employees and direct contractorsrequires access to GovDelivery, they cannot 'opt-out' of providing their PII as the user ID and password are used to log on to the system in order to perform their job duties.

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

All major system changes concerning PII are published via the System of Record Notice (SORN) for comment in the Federal Register as part of a modification of the applicable System of Record (SOR). This allows a 60 day comment period from members of the public.

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.

All PII within the system is provided directly by the individual. If a user does not believe their information should be in the system, they can contact GovDelivery Help Desk by either phone or email and the information will be removed for them. If they believe the information is inaccurate, they have the ability to modify the information themselves by login into GovDelivery. Subscribers only have access to their own 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.

Individual PII (email, name, and telephone number) is only modified by the individual who owns the PII and therefore cannot be inadvertently modified or destroyed by the system. Activities within the system are logged, so any changes to PII can be traced back to a specific time, and user providing non-repudiation within the system.

The system is highly available, ensuring the PII is available when needed. GovDelivery is located in a pair of Tier-1 datacenters to provide great availability. Hosting GovDelivery in two physically separate datacenters provide an avenue to ensure continuity of service to the public in a case of unforseen event.

The system automatically detects rejected email addresses, and removes those email addresses and all associated records from the system, ensuring that PII is accurate and up to date within the system.

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

Users:

Users/Subscribers have access to only their PII. Users use GovDelivery to communicate with the government.

Administrators:

Administrators/ Direct contractors have access to PII to facilitate the process of managing user accounts, creating new user accounts and disabling inactive user accounts. Administrators also have access to PII in order to maintain and test GovDelivery.

Contractors:

Administrators/Direct contractors have access to PII to facilitate the process of managing user accounts, creating new user accounts and disabling inactive user accounts. Administrators also have access to PII in order to maintain and test GovDelivery.

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

GovDelivery uses role-based access controls to ensure that administrators, and users are granted access on a ‘least privilege’ basis commensurate with their assigned duties (only those with the "need" to access the system are granted access for their assigned task/duties).

Administrators have access to PII as part of their day-to-day jobs. For Administrators, role-based access control is used for privileged role assignments. For these roles, the designated government contracting official or authorized representative designates and approves system Administrators. A request to add an Administrator is submitted in writing to the government contracting official or authorized representative and accounts are established in accordance with the access level required based on their role in the organization. It is left to the discretion of the designated CMS contracting official or authorized representative to determine the level of access an Administrator is granted.

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.

GovDelivery uses the principle of least privilege as well as role based access control to ensure system administrators and users are granted access on a "need-to-know" and "need-to-access" basis commensurate with their assigned duties.

Designated government contracting official or authorized representative designates and approves System Administrators. A request to add an Administrator is submitted in writing to the government contracting official or authorized representative and accounts are established in accordance with the access level required based on their role in the organization. It is left to the discretion of the designated CMS contracting official or authorized representative to determine the level of access an Administrator is granted.

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 direct contractors are required to take the CMS Information Security and Privacy training on an annual basis, or whenever changes to the training module are made. This training includes details on the handling of PII.

System administrators are required to complete role-based training and meet continuing education requirements commensurate with their role. Other training avenues such as conferences, seminars and classroom training provided by CMS/HHS is available apart from the regular annual training.

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.

User information will be disposed of (permanently deleted) when the service is no longer available. User preferences are also permanently deleted when a user unsubscribes and will be destroyed 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. This is based on NARA DAA-GRS-2013-0006-0003.

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

Designated government contracting official or authorized representative designate approves System Administrators. A request to add an Administrator is submitted in writing to the government contracting official or authorized representative and accounts are established in accordance with the access level required based on their role in the organization. It is left to the discretion of the designated CMS contracting official or authorized representative to determine the level of access an Administrator is granted.

GovDelivery is located in a pair of Tier-1 datacenters which provide physical control protections. The datacenters are physically secured with all exterior doors being locked and badges required for accessing the buildings. There are closed circuit cameras monitoring both the exterior and interior of the building. There are also security guards on duty during all hours of operation.

There are extensive training programs in place that repeatedly address Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH), privacy, and security. There are policies in place regarding the proper use of sensitive data, and all employees/contractors are fully aware of the penalties for misuse, whether intentional or unintentional. Peers are encouraged to report any violations or issues related to security and privacy events. All USB ports are locked to prevent usage of unauthorized devices.

GovDelivery is built using industry best practices and independently reviewed against Federal Information Security Management Act (FISMA) and National Institute of Science and Technology (NIST) Security and Privacy controls to ensure technical, operational, and management controls are properly applied.

Identify the publicly-available URL:

CMS.gov

CuidadoDeSalud.gov

Healthcare.gov

Medicare.gov

Questions.cms.gov,

Questions.Medicaid.gov

Questions.Medicare.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.

Web Beacons that 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?

Yes

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

Yes