US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/16/2016

OPDIV:

CMS

Name:

Next Generation Desktop-Medicare Beneficiary Portal

PIA Unique Identifier:
P-6855158-258143

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.
None

Describe the purpose of the system.
The purpose of the Next Generation Desktop (NGD) and Medicare Beneficiary Portal (MBP) is to provide general information to beneficiaries and future beneficiaries so that they can make informed Medicare decisions, maintain information on Medicare enrollment for the administration of the Medicare program including the following functions: ensuring proper Medicare enrollment, claims payment, Medicare premium billing and collection, coordination of benefits by validating and verifying the enrollment status of beneficiaries, and validating and studying the characteristics of persons enrolled in the Medicare program including their requirements for information.

This system tracks consumer interactions via the Call Center of the Health Insurance Exchanges (HIX) Program which includes Federally-facilitated Exchanges operated by CMS, CMS support and services provided to all Exchanges and state agencies administering Medicaid, Children Health Insurance Program (CHIP) and the Basic Health Program (BHP), and CMS administration of advance payment of premium tax credits and cost-sharing reductions.

The NGD and MBP will contain personally identifiable information (PII) about certain individuals who apply or on whose behalf an application is filed for eligibility determinations for enrollment in a Qualified Health Plan (QHP) through an Exchange, and for insurance affordability programs. Exchange functions that will utilize PII include eligibility, enrollment, appeals, payment processes and consumer assistance.

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

The NGD and MBP collect and store information about Medicare beneficiaries.
Access to Medicare beneficiary information requires callers and users of MyMedicare.gov to submit identifying information.

Beneficiaries provide the following information during the registration process to validate their identity: Medicare number, last name, date of birth, gender, zip code, employment status, phone number, relationship to the beneficiary, four (4) secret questions along with their answers, and email address. This information is validated against the Medicare Data Repository to confirm the user's information is valid upon the beneficiary entering their identifying information. Only the beneficiary's Medicare number, username, and e-mail address are stored in in the Next Generation Desktop/Medicare Beneficiary Portal system on a permanent basis in order to provide support.

The NGD will also maintain a caller history in case a customer service representative or CMS need to contact the beneficiary. The NGD and MyMedicare.gov systems also contain information related to Medicare enrollment and entitlement, group health plan enrollment data, as well as background information relating to Medicare or Medicaid issues. None of this information is shared outside of the NGD/MBP application.

Following successful registration, to access their beneficiary information on MyMedicare.gov, beneficiaries enter their unique user name and password.

PHI maintained within the NGD application includes: beneficiary enrollment, entitlement, eligibility information, and Medicare claims data.

Information collected by NGD/MBP for the system support staff, CMS employees and direct contractors, includes their username and business email address. Password information for beneficiaries and NGD/MBP supporting staff is stored within the Lightweight Directory Access Protocol (LDAP) as hashed strings. No password data is sent in clear text.

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

The Next Generation Desktop (NGD) and Medicare Beneficiary Portal (MBP) are Customer Relationship Management (CRM) systems. The NGD is the Customer Service Representative (CSR) desktop and was developed to handle inquiries for the 1-800- Medicare Helpline and Medicare Intermediary Contractors (Med A, Med B, Durable Medical Equipment) as well as the Affordable Healthcare Act Federally Facilitated Marketplace (FFM) Helpline. The NGD is designed to support the Virtual Call Center Strategy (VCS) initiatives of the CMS Office of Communications, Call Center Operations Group. The MBP is the internal CMS name for the MyMedicare.gov portal and is a web-based interface which allows Medicare beneficiaries to access their data via the Internet.

Beneficiaries provide the following information during the registration process to validate their identity: Medicare number, last name, Date of Birth (DOB), gender, zip code, employment status, phone number, relationship to the beneficiary, four (4) secret questions along with their answers, and email address. This information is validated against the Medicare Data Repository to confirm the user's information is valid. Only the beneficiary's Medicare number, username, and e-mail address are stored in in the Next Generation Desktop/Medicare Beneficiary Portal system on a permanent basis in order to provide support. None of this information is shared outside of the NGD/MBP application.

With a few minor exceptions, interactions are kept in the active NGD database for 3 years after the interactions are set to a status of “Done”. At that time, the completed interactions are purged. For calls, completing the interaction usually takes place within a minute or so of the person hanging up. MyMedicare.gov interactions also close right after a person logs off. Written correspondence and escalation activities can have a life span of up to 30 days and sometimes longer. The NGD and MBP send a record of all new and updated interactions each night. The National Data Warehouse (NDW) gets a record of all new and updated interactions each night. The NDW keeps these interactions for 10 years.

The National Data Warehouse (NDW), a separate CMS system with its own PIA for the information contained in it.

Information that is collected for the NGD/MBP support staff is stored until the staff member is no longer supporting the program. The NGD/MBP support staff, includes CMS employees and direct contractors, and the information is their username and business email address. Password information for beneficiaries and NGD/MBP supporting staff is stored within LDAP as hashed strings. No password data is sent in clear text.

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

Biometric Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Employment Status

Health Insurance Claim Number (HICN); Username, Password (hash), Medicare

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

Employees

Public Citizens

Patients

Providers, Suppliers, and Hospitals

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

PII of beneficiaries is used to create an account in the MBP and to access the account at future times.

The PII of NGD/MBP system support staff is used to access the functionality of the system.

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

Secondary uses of PII is for internal CMS application testing and training of the system for internal system support users.

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)), and OMB Circular A–123, Internal Control Systems, and Title 42 U.S.C. section 1395w– 21(d) (Pub. L. 105–3, the Balanced Budget Act of 1997).

Patient Protection and Affordable Care Act (PPACA) (Pub. L. 111–148) as amended by the Health Care and Education Reconciliation Act of 2010 (Pub. L. 111–152) collectively the Affordable Care Act. Title 42 U.S.C.18031, 18041, 18081—18083 and section 1414 of the Affordable Care Act.

The Medicare Modernization Act of 2013

5 U.S.C. Section 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.

1-800 Medicare Helpline (HELPLINE), 09-70- 0535. Published 5/12/2003 and updated 2/26/2008.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

Not applicable

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.

MyMedicare.gov users receive a confidential letter upon enrollment on the website. The letter provides their confidential password and an explanation of the system. The letter provides instructions should a Medicare beneficiary believe they were inaccurately enrolled in the system. As the Medicare Beneficiary Portal does not collect data and is only used as a portal to verify a beneficiary's information against other internal CMS systems, a process is not in place for MBP to notify a beneficiary that their personal information is collected.

The NGD/MBP system does not notify the system support staff users. They are notified as part of the general hire/onboarding process to work at CMS or have access to CMS information systems.

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.

For the NGD, there is no opt-out process because the beneficiary must provide some PII to receive accurate assistance. However, there is a ‘do not call’ feature that will prevent further contacting the beneficiary. The beneficiary simply requests this when speaking with a Customer Service Representative (CSR).

A beneficiary can prevent the information about the interaction from being associated with his or her Medicare records by refusing to provide a Medicare number or a name when calling. The call is then treated as a ‘contact’ call that comes from a member of the general public rather than a call about a specific beneficiary’s information. In these calls, the Customer Service Representative cannot gather or provide information to the caller about the beneficiary’s specific benefits, enrollments or claims.

If a Medicare beneficiary wants to create an account on the MBP/mymedicare.gov site, because it is required to establish their identity and create the account.

There is also no opt-out process for staff that support the NGD/MBP application. The PII is required to log into the areas of the system for which they have access.

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

MBP users receive a confidential letter upon enrollment on the website. The letter provides their confidential password and explanation of the system. The letter provides instructions to correct the account, should a Medicare beneficiary believe they were inaccurately enrolled in the system.

The MBP does not collect data and is only used as a portal to verify a beneficiary's information against other internal CMS systems, a process is not in place for MBP to notify a beneficiary that major changes have occurred to the system.

The users of the NGD are required to use Health Insurance Portability and Accountability Act (HIPAA) compliant disclosure procedures before disclosing any PII information about a Medicare beneficiary. The NGD tracks disclosure activities of the customer service representative.

Staff that support the NGD/MBP application are notified of any major changes that happen in the system that will require they provide additional PII via email or from their supervisor.

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.

For MyMedicare.gov users, they receive a confidential letter upon enrollment on the website. The letter provides their confidential password and an explanation of the system. The letter provides instructions should a Medicare beneficiary believe they were inaccurately enrolled into the system. Beneficiaries can also have their HICN disenrolled from MyMedicare.gov. A Help Desk has also been setup that beneficiaries can contact with any concerns regarding their account on the Medicare Beneficiary Portal.

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

There are Next Generation Desktop (NGD) quarterly releases where updates to mainframe systems are reflected within the NGD. Formal Software Development Lifecycle (SDLC) processes are leveraged including testing, User Acceptance Testing (UAT) and Independent Verification & Validation (IV&V). Other software technologies are in place to ensure no unexpected changes have occurred. This system does a crosswalk of PII data via an integration layer to the Common Working File (CWF) and is refreshed on a daily basis. User credentials for beneficiaries and NGD/MBP support staff are automatically reviewed by the system to determine whether or not the credentials are still valid. Accounts can be deactivated by either a user or a system administrator.

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

Administrators:

Some types of administrators (database, business analyst) may have access to PII to manage user accounts.

Contractors:

In their roles as administrators or call center employees, CMS direct contractors would have access to PII in accordance to the functions of those roles.

Others:

Call center CSRs have access to PII to service the calls from Medicare beneficiaries.

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

Access to NGD from a system integrator/contractor perspective is based on principles of least privilege. System administrators, network administrators, and developers do not have access to PHI, business analysts, and Siebel administrators access PHI only as required. Individual accounts which allow access to PHI at a system /programmatic level are reviewed annually and are authorized by management. All system integrator contractors complete security awareness and system access training prior to receiving initial access to the NGD. These individuals also receive annual refresher training.

CMS Customer Service Representatives (CSR’s) who access NGD to facilitate communication with Medicare beneficiaries receive security awareness training prior to being assigned a system role granting access to system data. CSR’s access PHI as a means of facilitating communication with Medicare beneficiaries who are communicating via: phone, web chat, or written correspondence. All access is granted through a defined access management process ensuring least privilege necessary access. Information is shared only on a need to know basis and at the direction of CMS.

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.

System users are assigned specific application and database views and responsibilities according to their specific usage of the system which limits the amount of PII that they may 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.

All CMS employees and direct contractors with access to CMS information systems are required to take an Annual Security and Privacy Awareness Training course. The completion is certified by an exam at the end of the course.

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

Role-based training is conducted for each user accessing the system. This training is acknowledged via the completion of training documentation prior to accessing the system.

Administrators with elevated privileges are required to complete additional security-specific training on an annual basis.

Additionally, the NGD National Site Administrator (NSA) and Local Site Administrators (LSA) attend training sessions conducted by the NGD Training team and must pass a certification exam prior to accessing NGD.

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.

The NGD and MBP follow the National Archives and Records Administration (NARA) N1-440-10- 07 Disposition which states that records are retained for up to 30 years for information on Medicare Part A payments. The other NARA General Records Schedules (GRS) that the system abide by are GRS 3.1, 3.2 and 4.3. The destruction of records varies, with the longest length of time being 7 years unless the records are required for other business, legal or investigative use.

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

The NGD and MyMedicare.gov systems secure PII via a multi-tiered architecture leveraging multiple types and layers of firewalls, intrusion detection technology and encryption of connections/access. Administrative controls include strict role-based access control, training of personnel and account review and auditing. The physical controls include the use of ID badges, pin numbers and key cards, video monitoring of the building and 24-hour security guards.

Identify the publicly-available URL:

https://mymedicare.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?

Yes