US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/02/2016

OPDIV:

CMS

Name:

National Data Warehouse

PIA Unique Identifier:

P-2786908-452998

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?

No

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 major system changes.

Describe the purpose of the system.

CMS implemented the National Data Warehouse (NDW) to serve as the central repository for capturing, aggregating, and analyzing information related to the Medicare beneficiary and consumer experience. NDW is the foundation for operational and management reporting, which improves the decision-making process, business practices, and services to beneficiaries. The data stored in the NDW is used to monitor, forecast, trend, analyze, and report on the performance of the Contact Center Operations (CCO) and all channels of communication that are available to the beneficiaries.

Primary users of the NDW are the CMS Office of Communications (OC), CMS Ombudsman, CMS Regional Offices (RO), CMS Center for Program Integrity (CPI), and Center for Medicare and Medicaid Innovation (CMMI).

Additional users include the CCO direct contractors General Dynamics Information Technology (GDIT), Training, Quality, and Content direct contractor (HighPoint Global), and the Next Generation Desktop direct contractor National Government Services (NGS).

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

In response to key Virtual Call Center Strategy (VCS) initiatives and Medicare reform legislation, CMS implemented the NDW to serve as the central repository for capturing, aggregating, analyzing, and monitoring information related to the beneficiary experience and to individuals and small employers exploring the Health Insurance Marketplace.

Beyond serving as a central repository, the NDW acts as a foundation for operational and management reporting to support improved decision-making, business practices, and services to contacts through all channels of communication. The data stored in the NDW is also used to monitor, forecast, trend, analyze, and report on the performance of the CCO contractors.

Seven CMS contractors; General Dynamics Information Technology (GDIT), Globo Language Solutions, HighPoint Global, National Government Services (NGS), Northrop Grumman Corporation (NGC), United Systems of Arkansas (USA Images), Inc., and Verizon, provide data inputs to the NDW. Information for 14 “family groups” of data is sent on a regular schedule through the CMS Enterprise File Transfer (EFT) infrastructure. The data files include Next Generation Desktop (NGD), Interactive Voice Response (IVR), and Total Quality Control (TQC) data. Due to data delivery time constraints, the CMS VCS Help Desk has been tasked by CMS with providing data delivery support to Verizon. Files are delivered early each day, enabling NDW Production to load files and produce reports within contractual time frames.

During the CMS contracted data provider's contact with beneficiaries, pertinent information such as Health Insurance Claim Number (HICN), name, address, city, state, ZIP code, phone numbers and date of birth is collected for generating statistics on beneficiary and consumer activities.

Access to the NDW is only available on CMSNet, the internal, private network hosted by CMS. Users (CMS employees and CCO direct contractors) are required to enter credentials, consisting of a user ID and password, in order to access the application. A formal user credential request process ensures that all users are approved by CMS to access NDW reports. A form is filled out during this user request which may collect user email address, desk phone number, desk location and name.

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

The NDW uses MicroStrategy Business Intelligence (BI) software through a web-based interface. The application server provides access to reports and analytics, and the database server stores information in an Oracle database that is not available for end user access.

Access to the NDW portal uses credentials provisioned through a CMS system. A valid login session is required before viewing the initial application menu. All users are either CMS Federal employees or their direct contractors. Information stored in the NDW is received from contracted data providers on a set schedule and includes information about beneficiary contact with the Contact Center through various channels such as 800-Medicare. All information received by the NDW application is provided through a secure file transfer mechanism using the CMS Enterprise File Transfer (EFT) Architecture.

Data providers include Verizon (Genesys Call Routing, Interactive Voice Response (IVR), Inbound Call Detail Traffic, Billing Records), HighPoint Global (Training, Quality and Content data), National Government Services (Next Generation Desktop activity, Web activity records, General Dynamic Information Technology ((GDIT) (Automated Call Distributor)), GLOBO Language Services (language translation services), and USA Images (printed material). Examples of reporting includes Average Hold Time (AHT), Average Speed of Answer (ASA), number of calls for each geographic area, and analysis of information used for contractor performance assessment.

Beneficiary information provided by CCO source systems list above is used by CMS to monitor and improve the beneficiary experience, and to help individuals and small employers exploring the Medicare Marketplace. Most Beneficiary contact is through the CMS Call Center staff (contractor CSR) and is used to improve CSR service and allow CMS to report on operations.

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

Other: NDW Application User Credentials (User ID and Password), HICN; employee desk location.

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

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

No

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

NDW serves as the central repository for capturing, aggregating, and analyzing PII information related to the Medicare beneficiary and consumer experience. PII information such as the address and phone number is used to aggregate information for analysis and improvement of Contact Center Operations services provided to the beneficiary.

System user PII is used to authenticate and gain access for system maintenance and system operations.

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

None

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

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

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.

All CCO source systems that provide data to the NDW are covered by this SORN.

09-70-0560 HIX (Health Insurance Exchange Program)

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

Not applicable for collection of user credentials.

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.

The NDW application does not directly collect information from individual Beneficiaries. The only personally identifiable information (PII) collected directly by the NDW application is the User Name and Password required at login. Notice is displayed before login (warning banner) indicating that information may be monitored, recorded, and audited. Acceptance of this statement is required by clicking "OK" before proceeding to the screen where PII (user name and password) is voluntarily entered. The application records every instance of user access.

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 NDW application does not directly collect information from individual Beneficiaries. The only personally identifiable information (PII) collected directly by the NDW application is the User Name and Password required at login. Entry of User Name and Password is voluntary, but required in order to login to the NDW application and access CMS data. CMS Acceptable Risk Safeguard (ARS) security policy requires that all access to systems containing CMS data (e.g. the NDW Application) must be controlled by an approved Access Control (AC) mechanism. User credentials are issued after a requestor submits an access form through the account request process. There is no option to opt-out or object to the information collection since CMS ARS required AC mechanisms must be satisfied before allowing access to CMS data.

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

The NDW application does not directly collect information from individual Beneficiaries. The only personally identifiable information (PII) collected directly by the NDW application is the User Name and Password required at login. Notice of changes to the application is provided to individuals by the NDW Help Desk by distributing the monthly NDW Bulletin Board. This document describes all changes to features and reports, outages notices, and provides training opportunities. The Bulletin Board is distributed by email, using the address provided during the account request process. If information were improperly disclosed, individuals would be notified using the same email mechanism.

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.

The NDW Help Desk is the central point of contact if an NDW Application user is concerned about the PII used to access the system. The NDW Help Desk is available through email or phone as published in the NDW Bulletin Board and within the NDW Application after login.

The NDW Help Desk logs all requests in the CMS Remedy system for assignment to the appropriate functional area. A ticket number is provided to the requester to track the activity through completion. Issues not adequately addressed by the NDW Help Desk can be addressed to the CMS Office of Communications, Contact Center Operations Group, through the VCS Help Desk (vcshelpdesk@vcshelpdesk.com or 866-804-0685, option #2).

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

PII entered by NDW Application users to validate access is reviewed every month as documented in the MicroStrategy License Review Process Standard operating Procedure (SOP). The SOP describes activities completed by the NDW Security Officer to ensure that integrity, availability, accuracy, and relevancy of account information. The application request process is reviewed and each created, modified, and deleted account is logged to verify that actions were completed as described in support process documentation. Accounts are reviewed tri-annually to ensure that inactive accounts are removed in compliance with CMS ARS. The NDW Security Officer reviews NDW Help Desk requests that pertain to access requests. Report of this regular review are provided to CMS through a Weekly Technical Dashboard.

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

Users:

The purpose of this system is to track the nature of customer service interaction. All levels of users require access to the customer interaction data to troubleshoot issues or to provide analysis. Users have access to PII to execute reports that provide information about caller interactions and produce reports such as Average Hold Time (AHT), Average Speed of Answer (ASA), or analysis of questions based on regional area.

As previously noted, NDW application users include CMS Federal employees and direct contractors.

Administrators:

Administrators can execute reports/queries to assess the performance of the application and to troubleshoot issues. Due to the nature of their access, direct queries against the database could yield PII.

Developers:

Similar to Administrators, Developers can execute reports and queries to verify the validity of new/updated report and queries. Due to the nature of their access, they can use application tools to direct query and validate reports.

Contractors:

The purpose of this system is to track the nature of customer service interaction. All levels of users require access to the customer interaction data to troubleshoot issues or to provide analysis.

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

Role-based access is applied to enforce least privilege rights to system users, and therefore access to PII. This includes Users, Administrators (including Operating System, Applications, and Database administrators), and Developers as described in Question 31. CMS sets guidelines for access to the Development and Production contractors in the NDW application Statement of Work (SOW) and approves role-based access for all administrators and developers.

If the NDW Development (direct) Contractor determines that additional system roles are required, the purpose and scope of the new role are defined and approved by the CMS COR. The NDW System Security Plan (SSP) contains a list of CMS approved roles.The NDW Security Officer reviews the roles and role membership each quarter to ensure compliance and documents the activity in the Weekly Technical Dashboard to record compliance.

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.

All NDW users are assigned to security groups that limit report type and data access the Role-based access enforces least privilege.

Examples include the Medicare Administrative Contractors (MAC), who are only able to access data specific to their area of responsibility. The system is partitioned to allow only data require by a user is available.

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 users are subject to CMS' Rules of Behavior that define responsibilities for using CMS systems. CMS requires that all users complete annual Computer Based Training (CBT) for System Security and Privacy Awareness Training.

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

To meet CMS Minimum Security Requirements (CMSR) standards, all NDW application users are provided training based on job duties and application access requirements. Administrators (e.g. operating system, application, and database) with elevated privileges are required to complete eight hours of security specific training each year.

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 retention policy for this system is specified in NARA Guidance for Patient Protection and Affordable Care Act - Private Health Insurance Systems section 8 - Cutoff annually. Destroy 7 years after cutoff.

Disposition Authority: DAA-0440-2012-0005-0013.

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

PII in the NDW database is protected through layers of security. This includes administrative controls over issuing accounts to end users and system administrators for access to the application and operating system. Firewall and data network access controls enforce technical controls that limit inter-service process connections to predefined devices and ports. Physical access controls in the data center hosting the NDW application include electronic door locks and monitoring, video cameras, and daily testing of access and environmental controls.

Administrative controls are verified through an independent audit function. This includes monthly reviews of system access changes and license reviews. The audit function is performed by a direct contractor separate from the Production direct contractor to ensure independence.