US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/15/2017

OPDIV:

CMS

Name:

Chronic Condition Data Warehouse

PIA Unique Identifier:

P-5754498-529482

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.

N/A

Describe the purpose of the system.

The Chronic Condition Warehouse was designed for the Centers for Medicare & Medicaid Services to support research, policy analysis, quality improvements, and demonstrations using Medicare/ Medicaid patient level information linked across all claims, eligibility data, nursing home, home health assessments, and CMS beneficiary survey data. The purpose of this system is to collect and maintain a person-level view of identifiable data to establish a data repository to study chronically ill Medicare beneficiaries. This system utilizes data extraction tools to support accessing data by chronic conditions and process complex customized research data requests related to chronic illnesses.

The data collected and maintained in this system are retrieved from the following databases which are covered under their own PIA: Medicare Drug Data Processing System, Medicare Beneficiary Database, Medicare Advantage Prescription Drug System, Medicaid Statistical Information System, Retiree Drug Subsidy Program, Common Working File, National Claims History, Enrollment Database, Carrier Medicare Claims Record, Intermediary Medicare Claims Record, Unique Physician/Provider Identification Number, Medicare Supplier Identification File, a Current Beneficiary Survey, National Plan & Provider Enumerator System, Long Term Care Minimum Data Set (MDS), home health agencies (HHA) Outcome and Assessment Information Set, and Integrated Data Repository.

The Chronic Condition Warehouse (CCW) system supports three scopes of work: the CCW system, the Research Data Distribution Center that supports the dissemination of research data, and the Virtual Research Data Center (VRDC). These provide a secured environment and research tools for authorized users to access data from the warehouse. Researchers request extracts of data from the Centers for Medicare and Medicaid Services.

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

The Chronic Condition Warehouse (CCW) maintains administrative use and claims data that includes personally identifiable information (PII) and protected health information (PHI) on patients and providers participating in Medicare and Medicaid programs. The PII and PHI includes: Provider Name, Provider Number, Unique Provider Identification Number, National Provider Identifier Number, Name, Mailing Address, Telephone Number, Gender, Race, Ethnicity, Social Security Number (SSN), Date of Birth, Military Status, Taxpayer ID, Medical Notes, Medical Records Number, Medical Claims Data, Health Insurance Claim ID, and Date of Death. Other PII includes: User Credentials (UserID and Password).

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

The primary purpose for the Chronic Condition Warehouse (CCW) use of the information it collects, uses and maintains is to establish a data repository to study chronically ill Medicare beneficiaries. This system utilizes data extraction tools to support accessing data by chronic conditions and processes complex customized research data requests related to chronic illnesses.

The CCW collects and maintains user's credentials in order to control and authenticate access to the system. The users consist of external customers, as well as, internal support staff (CMS employees and direct contractor).

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

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Military Status

Taxpayer ID

Other: Medical Claims Data, Provider Number, National Provider Identifier Number, Health

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

Employees

Public Citizens

Patients

Providers

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

This system will utilize data extraction tools to support accessing data by chronic conditions and process complex customized research data requests related to chronic illnesses. Information retrieved from this system may be disclosed to: Support regulatory, reimbursement, and policy functions performed within the agency or by a contractor, grantee, consultant or other legal agent; assist another Federal or state agency with information to contribute to the accuracy of CMS's proper payment of Medicare benefits, enable such agency to administer a Federal health benefits program, or to enable such agency to fulfill a requirement of Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds; support an individual or organization for a research project or in support of an evaluation project related to the prevention of disease or disability, the restoration or maintenance of health, or payment related projects; support Quality Improvement Organizations (QIO); support litigation involving the agency; and combat fraud and abuse in certain Federally-funded health benefits programs.

The user's credentials is used to authenticate user's of the system for access control purposes.

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

N/A

Describe the function of the SSN.

The SSN is used to create an encrypted beneficiary identifier which is used in place of the SSN on all extracted data from the warehouse.

Cite the legal authority to use the SSN.

Medicare Prescription Drug, Improvement, and Modernization Act of 2003. (Section 723); Social Security Act (Title XVIII)

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

Affordable Care Act, 45 CFR 155.210(e); Patient Protection and Affordable Care Act; Section 723 of the Medicare Prescription Drug Improvement and Modernization Act of 2003

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.

09–70–0573 - Chronic Condition Data Repository

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

N/A

Is the PII shared with other organizations?

Yes

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

Within HHS

To Quality Improvement Organizations (QIO) in connection with review of claims, or in connection with studies or other review activities conducted pursuant to Part B of Title XI of the Act, and in performing affirmative outreach activities to individuals for the purpose of establishing and maintaining their entitlement to Medicare benefits or health insurance plans.

Other Federal Agencies

Department of Justice for Data Use Agreement Fulfillment, Research, Fraud and Abuse

State or Local Agencies

State agencies to assist Medicaid programs within the state; for Data Use; Agreement Fullfillment, Research, Fraud and Abuse

Private Sector

To an individual or organization for a research project or in support of an evaluation project related to the prevention of disease or disability, the restoration or maintenance of health, or payment related projects; Data Use Agreement Fulfillment, Research.

To Quality Improvement Organizations (QIO) in connection with review of claims, or in connection with studies or other review activities conducted pursuant to Part B of Title XI of the Act, and in performing affirmative outreach activities to individuals for the purpose of establishing and maintaining their entitlement to Medicare benefits or health insurance plans.

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

Interconnection Agreement (ISA) between CMS/CCW information system and Symantec

Interconnection Agreement (ISA) between General Dynamics Information Technology – Towson Office and WAN Services-CMSNet-Verizon (CMSNet)

Interconnection Agreement (ISA) between General Dynamics Information Technology – Warrenton Office and WAN Services-CMSNet-Verizon (CMSNet)

Interconnection Agreement (ISA) between General Dynamics Information Technology – West Des Moines Office and WAN Services-CMSNet-Verizon (CMSNet)

Describe the procedures for accounting for disclosures.

The CCW has a multitude of Data Use Agreements (DUA) that are used to track the data that is disclosed to it's recipients. The DUA tracks who the data is received by, for what purpose, and the date it was disclosed. Every Qualified Entity receiving data must have an agreement with CMS in the form of an Information Exchange Agreement or contract with all security and privacy requirements included. A DUA must be completed by the person receiving CMS data in accordance with current CMS policies.The Privacy Act of 1974 (5 U.S.C. § 522a) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule (45 C.F.R Parts 160 and 164), allows CMS to disclose information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such compatible use of data is known as a ''routine use.'' The proposed routine uses in this system meet the compatibility requirement of the Privacy Act.

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 data collected and maintained in this system are retrieved from the following databases which are covered under their own PIA: Medicare Drug Data Processing System, Medicare Beneficiary Database, Medicare Advantage Prescription Drug System, Medicaid Statistical Information System, Retiree Drug Subsidy Program, Common Working File, National Claims History, Enrollment Database, Carrier Medicare Claims Record, Intermediary Medicare Claims Record, Unique Physician/Provider Identification Number, Medicare Supplier Identification File, a Current Beneficiary Survey, National Plan & Provider Enumerator System, Long Term Care MDS, HHA Outcome and Assessment Information Set, and Integrated Data Repository. The process to notify individuals that their PII will be collected is the responsibility of these systems.

System users are not notified that their personal information will be collected as login credentials are necessary to access the CCW system. A system banner is presented upon entering a user's credentials.

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.

System users do not have an option to opt out as login credentials are necessary to access the CCW system.

The data collected and maintained in this system are retrieved from the following databases which are covered under their own PIA: Medicare Drug Data Processing System, Medicare Beneficiary Database, Medicare Advantage Prescription Drug System, Medicaid Statistical Information System, Retiree Drug Subsidy Program, Common Working File, National Claims History, Enrollment Database, Carrier Medicare Claims Record, Intermediary Medicare Claims Record, Unique Physician/Provider Identification Number, Medicare Supplier Identification File, a Current Beneficiary Survey, National Plan & Provider Enumerator System, Long Term Care MDS, HHA Outcome and Assessment Information Set, and Integrated Data Repository. The process to offer the ability to opt-out to individuals whose PII will be collected is the responsibility of these systems.

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

The data collected and maintained in this system are retrieved from the following databases which are covered under their own PIA: Medicare Drug Data Processing System, Medicare Beneficiary Database, Medicare Advantage Prescription Drug System, Medicaid Statistical Information System, Retiree Drug Subsidy Program, Common Working File, National Claims History, Enrollment Database, Carrier Medicare Claims Record, Intermediary Medicare Claims Record, Unique Physician/Provider Identification Number, Medicare Supplier Identification File, a Current Beneficiary Survey, National Plan & Provider Enumerator System, Long Term Care MDS, HHA Outcome and Assessment Information Set, and Integrated Data Repository.

The process to notify and obtain consent from individuals that their PII will be used for a different purpose fromwhat it was initially collected for is the responsibility of these systems.

A change in the mission of the Chronic Condition Warehouse would also be accompanied by a revision to the system or record notice (SORN) in the Federal Register for a public comment period.

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.

Resolution for any concerns regarding the inappropriate use or disclosure is addressed by the CCW Help Desk or the CMS Help Desk.

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

Data files are loaded into the Chronic Condition Warehouse on a periodic basis from the other CMS databases. Any corrections in the original collection will be propagated into the Chronic Condition Warehouse up until the final cutoff date for the data set. Routine reviews and automated database integrity checks are used to maintain the integrity of the data while in the Chronic Condition Warehouse.

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

Users:

Users authorized under a Data Use Agreement may access personally identifiable information to conduct research

Administrators:

System administrators may access personally identifiable information to manage system and troubleshoot potential issues.

Developers:

Developers may access personally identifiable information in the process of managing and preparing data sets and data extracts.

Contractors:

Direct contractors authorized by the Centers of Medicare & Medicaid Services may access personally identifiable information to conduct research under the assigned contract.

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

Access to Chronic Condition Warehouse is approved by Centers for Medicare & Medicaid Services, Account Access (CAA). Access is granted using the principle of least privilege, users are only granted access to PII, PHI based on their job responsibilities needed to perform their job. Role creation involves an analysis for the role definition and type of access, periodic access attestations are conducted to ensure the level of access is maintained for each of the roles.

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.

Users are granted access based on their job duties and permissions are established based on their approved job codes assigned to their user IDs. CCW performs security controls access levels via roles and conducts periodic access attestations.

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.

The Centers for Medicare & Medicaid Services requires all employees and direct contractors to undergo annual Security Awareness Training in order for each user to maintain their access to the system. General users of the Chronic Condition Warehouse are required to complete security awareness training to obtain an account. Courses typically assigned to the general users: Annual Security Briefing, Security Awareness Training, HIPPA Privacy Training, Risk Management, Ethics and Business Conduct, Privacy and Security of Personal Information.

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

The Chronic Condition Warehouse Maintainer undergoes additional role based training specific to the targeted roles of Program and Business Managers, System Administrators, and Developers. Below is a sample list of role based courses:

Waterfall and CMS Expedited Life Cycle; Configuration Management; Architecture and Development Introduction to System Development Life Cycle; Incident Communications; Data Loss Incident Management Best Practices

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 Chronic Condition Warehouse (CCW) has a National Archives and Records Administration (NARA) Records Disposition Authorization, DAA-0440-2012-0013-0001, which states that records containing PII are destroyed 30 years after cutoff (annually).

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

The Chronic Condition Warehouse uses National Institute of Standards and Technology (NIST), approved encryption tools for encrypting protected health information or personally identifiable information data files. A data-masking technique is applied to the beneficiary identifier for all PII and PHI included in a data request. PII and PHI files are encrypted. The decryption password is electronically mailed only to the person identified as the recipient of the data.

CCW uses an approved courier service (with tracking receipt) to deliver all data extracts containing identifiable data. Deliveries require signature, and email confirmation of receipt is requested. The Data Center undergoes annual security assessment and authorization. Physical and environmental controls include: Badging, Loading dock staging area, Operating Area Access Agreements, and Surveillance Monitoring.

Identify the publicly-available URL:

https://ccwdata.org

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 uner 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