US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/06/2021

OPDIV:

CMS

Name:

Centralized Data Exchange

PIA Unique Identifier:

P-7097612-776726

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.

Agency

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.

Alteration in Character of Data

Describe in further detail any changes to the system that have occurred since the last PIA.

CDX will store SSN due to onboarding model teams requirement.

Describe the purpose of the system.

Centralized Data Exchange (CDX) enables interoperability and provides center-wide data collection capabilities. The exchange solution will support sending the right data, at the right time, sending the right amount, and referencing the right participants. CDX application will create a complete data access that enhances integration with open secure application programming interface (API) to enable better ways of interacting with partners (APIs, electronic health record [EHR], and various Health IT distribution channels).CDX solution will be built upon a robust cloud base platform that will collect Big Data and aide in the progression of this data into Intelligent Digital data in Health IT standards.

This progression will support data liquidity and third-party app integration with Certified EHR Technology (CEHRT); thus producing a refinement of clinical evidence based on quality clinical data captured through care delivery and this will support the mission of Center for Medicare andMedicaid Innovation (CMMI) to positively drive the reform of healthcare in America.

The CDX solution vehicle will contribute technical expertise to CMMI's Front Office in support of the rollout of interoperability rule. The design of the CDX solution will allow data driven, value-based care support to model teams so they can include interoperability in the model design, review the model flow and show how data sharing can help drive change.

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

Types of data collected can include administrative and medical records, Emergency Medical Services (EMS) data, claims data, vital records, surveys, attestations, names, medical notes, date of birth, medical record numbers, Social Security Number (SSN), and other health related data.

CDX will collect, store and maintain all data that is uploaded to CDX. The user can delete the files from the User Interface, but the information will be retained in the database until it is archived per the data retention policy. All users will only have access to data that they originally uploaded into CDX or was shared with them by a user that had access to that data in CDX. A user's ability to share data that was shared with them and not originally posted by themselves, will be determined on their user role.

Data will be stored in accordance with each reliant model's needs and allow participants to submit data through multiple formats. All models will be able to share data through CDX through its sharing capability.

CDX utilizes user ID and passwords and these login credentials are used to grant access to the system. Users of CDX are the system administrators, maintainers and developers, and direct contractors. The login credentials (user ID) used to access CDX are provided to users by CMS enterprise identity management system.

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

Currently CMMI has duplicative file upload/download features across many systems. These existing features are lacking in terms of performance, capacity, and reliability. CDX provides both familiar drag-and-drop based file sharing and standard -based API driven centralized data exchange capabilities. CDX system utilizes a user interface (UI) to enable users to perform modern ad-hoc exchanges and APIs to exchange data via fast healthcare interoperability resources (FHIR) and other APIs according to the interoperability rules of the Affordable Care Act. CDX provides the capability to replace the current file upload/download features embedded into individual systems with one centralized CMMI file exchange solution.

CDX purpose is to provide greater performance, capacity, and reliability across the entire CMMI environment. PII including but not limited to Name, Medical Notes, EMS data, Date of Birth, Social Security Number (SSN), and Medical Records Number is stored in and shared through the service that CDX provides to those with access.

CDX uses PII to retrieve system records, pertaining to patients, including using the Data of Birth, and Medical Record Numbers.

Login credentials are provided by CMS's enterprise identity management system and used to grant access to the system. The primary consumer of the CDX service is the Model Team and Model Participants. Users of CDX are the Model teams/participants, CDX privileged user role, CDX general user role users, system administrators, maintainers and developers.

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

Medical Records Number

Medical Notes

Other: Medical Records, Claims Data, Vital Records, EMS Data, Other Health Related Data

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

Public Citizens

Patients

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

PII is primarily used for Beneficiary Identification.

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

N/A. CDX does not utilize PII for any other purposes.

Describe the function of the SSN.

CDX will store the Social Security Number (SSN) which is utilized to conduct probabilistic matching with data in the National Emergency Medical Services Information System (NEMSIS) standard. Emergency Medical Services (EMS) follow the NEMSIS standard to collect data resulting from an emergency 911 call for assistance. NEMSIS standard data includes SSN, details of the Patient, Exam, Disposition, Labs, Medications, and other related data. CDX transfers data extracts to authorized stakeholders that allows them to analyze the data to determine the efficacy of the model and its operation. CDX, through Role Based Access Control (RBAC), ensures that authorized users shall only have access to the last four digits of the SSN.

Cite the legal authority to use the SSN.

Affordable Care Act (ACA) Sec. 3021

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

Affordable Care Act (ACA) Sec. 3021

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.

Master Demonstration, Evaluation and Research Studies for ORDI, SORN 09-70-0591, Pub.

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

N/A. Information is not collected directly from the individual.

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 information that is submitted is sourced from existing medical records that have already been collected by the provider. Responsibility for patient notification resides at the point of information collection from the individual. However, all Medicare participants are provided with a Notice of Privacy Practice that states that although they can elect to not share data for certain processes, as a condition of participating in Medicare, their information will be shared for certain purposes, such as quality assessment and reporting.

CDX user’s authentication is provided by CMS's enterprise identity management system and used to grant access to the system.

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 information that is submitted is sourced from existing medical records that have already been collected by the provider. Responsibility for patient opt-out process resides at the point of information collection from the individual. The provision of PII is "voluntary" as that term is used by the Privacy Act.

All system user login credentials are provided by CMS's enterprise identity management system and used to grant access to the system.

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

The information that is submitted is sourced from existing medical records that have already been collected by the provider. Changes to CDX that would involve changes in uses and disclosures of beneficiaries' PII are not expected to occur. In the event that such changes were to occur, CMS will inform individuals using multiple channels, including direct mailings; notices on the CMS website (including edits to CMS's posted privacy policy), or changes to the relevant systems of records notices. Changes involving uses and disclosures of authentication information are also not expected to occur. In the event of such changes, employees will be notified by notices on the CMS intranet; newsletters; updates to the relevant systems of records notices; e-mails to affected individuals; and through supervisors and system owners.

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 information that is submitted is sourced from existing medical records that have already been collected by the provider.

Responsibility for patient concerns regarding the use of PII resides at thepoint of information collection from the individual.

If an individual has concerns that their PII has been inappropriately obtained, used, or disclosed or that the PII is inaccurate, the following procedures should take place: If the user believes an incident has occurred, the user should cease what they are doing and notify Model Specific Helpdesk. The Help Desk will create a ticket and will notify CDX Management and CDX Security team. CDX security team will investigate the event.

If reportable, security will notify the CMS Help Desk within 1 hour of the incident occurring. (If the event is unreportable, security will notify the Help Desk to close the ticket). The CMS Help Desk Representative will serve as the CMS First Respondent in documenting and assessing the incident to ensure that the incident has been contained. The incident will be escalated and routed to the appropriate CMS group per CMS Incident Response Policy to determine the severity and course of action for mitigation. System user's credential information is collected via registration with CMS's authentication system; therefore, no process exists within CDX to address these concerns. Any perceived issue should be reported to the CMS Help Desk and escalated to the CMS authentication system administrators.

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 IS2P2 requires business owners to Conduct initial evaluation of PII/PHI holdings and review holdings annually to ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete and reduce PII holdings to the minimum necessary for the proper performance of the documented CMS function for all information systems containing PII/PHI. Data availability is protected by security controls selected as appropriate. CDX follows the CMS Security and Privacy program and complies with the CMS Acceptable Risk Safeguards, and National Institute of Standards and Technology (NIST) documents such as its Special Publications to select controls appropriate to the level of risk of the system, determined using NIST's Federal Information Processing Standard 199.

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

Users:

Each user should have access to their own PII, to perform tasks relating to their own account.

Administrators:

Administrators are responsible for assigning user roles to user accounts. As such, they may be exposed to user's PII.

Contractors:

Direct contractors who have system administration roles may also be exposed to the user's PII that is stored in the system as part of their approved responsibility.

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

User roles are established and managed in a way to ensure that users are only able to access data that pertains to their own organization. Roles are assigned and access is granted, to CDX and the PII it contains, based upon principle of least privilege and "need-to-know" or "need-to-access" requirements to perform their assigned duties.

System Administrators review user accounts at least semi-annually. Any anomalies are addressed and resolved by contacting the user, or by removing their access if no longer required. Activities of all users are logged and reviewed by the system administrator to identify abnormal activities, and if any are found they are reported to the business owner, and the ISSO.

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.

The system enforces role-based access controls, based on a least privilege model, to enforce theprotection of data from unauthorized personnel. The application controls data access, such that the organizational user will be restricted to only access the data pertaining to their own organization.

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 complete mandatory security and privacy awareness training prior to gaining access to the CMS Network. Each year, thereafter, the user must get recertified. In the event they fail to complete the recertification training, the user's access will be terminated.

All CDX end-users will be provided notification at the commencement of each session, to make them aware of their responsibilities for protecting the PII/PHI information being shared, collected and maintained.

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

CMS also requires CMS employees and direct contractors, on an annual basis, to complete Role Based Training and HHS Records and Retention Training. Employees are also required to complete Annual Refresher Training, Insider Threat Training, and OWASP Training (exclusively for the project team i.e. developers, testers, & BAs).

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 application adheres to data retention and destruction policies/procedures that follow National Archives and Record Administration (NARA) guidelines related to data retention and NIST guidelines related to data destruction. More specifically, CDX adheres to the following NARA general records schedule guidelines:

DAA-0440-2015-0007-0001; Destroy no sooner than 10 year(s) after cutoff but longer retention is authorized and DAA-GRS-2013-0005-0003, 5 year retention.

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

To secure PII, CDX follows, and the direct contractors are bound by contract to follow, the CMS Security and Privacy program and complies with the CMS Acceptable Risk Safeguards which are aligned to Health and Human Services (HHS) policies and to NIST requirements. CDX PII is secured with security controls as required by the CMS Security Program.

Administrative: Users are provided with privacy training to understand how to properly handle and disclose privacy data. The system uses the principle of least privilege as well as a role based access control to ensure system administrators, and users are granted access on a "need-to-know" and "need- to- access" commensurate with their assigned duties. Users must receive manager approval to gain access to the system.

Technical: The data in CDX is secured behind a various infrastructure and through application security controls. Technical security controls include, but are not limited to audit controls, user accounts, passwords, and access limitation. All data at rest in CDX is encrypted with a FIPS 140-2 compliant encryption algorithm.

Physical: The Data Center, hosting the application, has security guards and controlled access rooms with locks to guard against unauthorized access.