US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/24/2025

OPDIV:

CMS

Name:

Beneficiary Claims Data API

PIA Unique Identifier:

P-4191291-918843

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

Significant System Management Change

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

Data at Point of Care is releasing an onboarding Portal for Providers and application developers working for Providers, known as Authorized Officials (AOs) and Credential Delegates (CDs) respectively.

Minimal new Personal Identifiable Information (PII) will be stored and processed related to AO and CD user identities.

There are no privacy changes to Claims Data storage, maintenance, nor processing.

Describe the purpose of the system.

The document’s references to Beneficiary Claims Data Application Programming Interface (API) (BCDA) are intended to be inclusive of the program’s component parts: Accountable Care

Organization (ACO) API, Data at Point of Care (DPC) API and Claims Data to Part D Sponsors (AB2D) API, unless otherwise noted. The ACO API also includes the System-to-System Authentication Service (SSAS).

ACO API is meant to allow ACOs easier access to claim and claim line data about the beneficiaries who have been assigned to their practitioners for care. Currently, the highly manual process ACOs use to access this data is a hindrance to beneficiary care, ACO API seeks to make this information more easily accessible to help ACOs and the practitioners that work with them have a fuller understanding of what's happening in beneficiaries' lives sooner.

Centers for Medicare & Medicaid Services (CMS) provides this information today through the Accountable Care Organization - Operational System (ACO-OS) in the form of a Claims and Claim Line Feed (CCLF) download via Electronic File Transfer mailboxes. ACO API delivers the data in a structured format that allows easier and more accurate processing with less effort required by the beneficiary.

The AB2D API securely provides stand-alone Part D Plan (PDP) Sponsors with Medicare Parts A and B claims data for their active enrollees. Sponsors will be able to utilize this claims data to promote the appropriate use of medications and to improve health outcomes for their beneficiaries. AB2D also implements the Fast Healthcare Interoperability Resources (FHIR) standard.

DPC API is meant to allow healthcare providers better access to a beneficiary's Medicare claims data. As beneficiaries move throughout the healthcare system, providers often struggle to gain and maintain a complete picture of their medical history. The DPC project fills in the gaps with claims data to inform providers with structured patient history, past procedures, medication adherence, and more. Like ACO and AB2D APIs, DPC implements the FHIR Bulk Data Access specification, which provides an asynchronous interface over the existing Blue Button Beneficiary FHIR Data (BFD) Server data model.

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

The information in BCDA systems includes beneficiary name, address, email, phone number, birth date, sex, race, claim information, and a Medicare Beneficiary Identifier (MBI).

DPC does an element comparison against a valid Login.gov identity and the role of a Provider's Authorized Official in Provider Enrollment, Chain, and Ownership System (PECOS). SSN is the data element utilized for this role verification, only for Login.gov (Identification Assurance Level) IAL2 Provider Authorized Officials, which is not collected, stored nor maintained by DPC or BCDA systems.

Other data handled includes inpatient, outpatient, and pharmacy claims, including diagnoses, procedures, preventative tests, and medications. In addition, it includes data for outpatient care, hospital admissions, emergency room care, and urgent care. The underlying data model is provided by the Beneficiary FHIR Data (BFD) Server.

Production DPC API access is managed via administrative dashboard -- a component part of the DPC API project. BCDA team members administer accounts for individuals, the organizations they are part of as well as API credentials associated with said organizations.

AB2D, ACO and DPC APIs provide FHIR-formatted bulk data files to PDP Sponsors, ACOs and healthcare providers for their assigned and active beneficiaries respectively. Data at the Point of Care does not require individual beneficiary authorization, unlike the ACO API, but will allow a process for beneficiaries to opt out of data sharing.

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

Medicare beneficiary information (in the form of FHIR Patient, Coverage and Explanation of Benefit resources) is made available via a secure API to API clients based the beneficiaries attributed to the ACO (ACO API), healthcare provider (DPC API) or stand-alone PDP sponsors (AB2D API). Retrieval of records from the BFD Server will be done using an MBI, which is stored within BCDA systems on a permanent basis.

In the case of DPC API, healthcare providers are required to submit patient rosters identifying the beneficiaries for which they are entitled to receive data for treatment purposes under HIPAA. Patient rosters include patient name, sex, date of birth, address, phone number and MBI. In addition, healthcare providers must submit information regarding practitioners, including practitioner name, sex, address and National Provider Identifier (NPI). This information is stored by DPC API on a permanent basis.

Developers that wish to use ACO, DPC and AB2D APIs must follow standard on-boarding procedures with CMS. For those developers we store name, email address, organization, and credentials.

In the case of ACO API, developers may only be individuals from an active ACO. For DPC API, developers can be CMS employees, CMS direct contractors, or third-party developers in association with a vetted healthcare provider. For AB2D, PDP sponsors assign an "AB2D Data Operations Specialist" that has authority to access and view data provided by the API.

Requests to BCDA systems are made by API clients for a bulk data export housed in the BFD Server. An API client’s request for bulk data export is recorded as a job and tracked by a job queue. As a job is processed, requests are made to the BFD Server and responses collated into bulk export files. When a job is complete, data is made available for download by API clients.

DPC does an element comparison against a valid Login.gov identity and the role of a Provider’s Authorized Official in Provider Enrollment, Chain, and Ownership System (PECOS). SSN is the data element utilized for this role verification, only for Login.gov (Identification Assurance Level) IAL2 Provider Authorized Officials, which is not collected, stored nor maintained by DPC or BCDA systems.

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
Medical Records Number
Medical Notes
Other: Medicare Beneficiary Identifier (MBI) CMS Credentials, Race, Sex

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors
Patients
Healthcare providers

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

ACO API delivers information about Medicare beneficiaries to ACOs to enable data analysis tasks related to the services beneficiaries receive through said ACOs.

AB2D API gives PDPs claims data to Part D Sponsors per requirements set forth in the Bipartisan Budget Act of 2018 now Public Law No: 115-123. The AB2D API uses PII to provide accurate beneficiary data to the authorized user that requests it. Beneficiaries can opt out of having their data shared by calling 1-800-MEDICARE. AB2D receives this information from BFD as its source of truth.

DPC API provides FHIR-formatted bulk data files to fee-for-service providers for their active patients as needed for treatment purposes under HIPAA. Data is shared for covered entities for treatment purposes as defined under HIPAA. Patients can choose to opt out of data sharing.

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

Provider email address is used for User Acceptance Testing.

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

Section 1874(a) and 1875 of the Social Security Act and 5 USC 301.

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.

General Services Administration (GSA)/TTS-1 Login.gov (GSA)

09-70-0555 National Plan and Provider Enumeration System (NPPES)

09-70-0532 Provider Enrollment, Chain, and Ownership System (PECOS)

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Other
Government Sources
Within the OpDiv
Other
Non-Governmental Sources
Other

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.

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

ACO API: Each ACO is authorized by its respective CMS Center, normally via a Data Use Agreement (DUA) or Attestation/Authorization executed between CMS and the ACO, and Information Security Agreements between CMS and the ACO.

AB2D API: PDPs must attest for each contract within HPMS to be eligible to receive current claims data. Only authorized PDPs may request, access, and use the exported data from the API. The data belongs to the sponsors and is simply processed and served by the AB2D API.

DPC API: to receive data from the DPC application, a healthcare provider must have a treatment related purpose for viewing a patient's claims history. Providers attest to their treatment purposes by submitting an attribution roster which lists the patients currently under their care.

Describe the procedures for accounting for disclosures.

AB2D API: The business owners are responsible for the PDPs maintaining a process for distribution of the data delivered. Additionally, the PDPs are responsible for maintaining proper attestation status within HPMS otherwise they will lose access to the data. All access is controlled and audited within Okta and can be cross referenced for accountability. This data is only disclosed to relevant parties. Job records are kept within the AB2D database.

ACO API: The business owners responsible for the ACO have existing processes for distribution of the CCLF files to the ACOs. ACO API relies on those existing procedures and augment them with system level auditing of requests and deliveries of data to the ACOs.

DPC API: Providers requesting data are bound to the Terms of Service (ToS) and have existing processes for use of data exported from the BFD service. DPC relies on these existing procedures and augments them with system level auditing of requests and deliveries of data to the providers.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Not Applicable for beneficiary claims data. Notice is the responsibility of the CCW and IDR systems.

The developer access credentialing process, as part of the BCDA systems' on-boarding processes for accessing BCDA system environments, provides notification to the developers prior to the collection in the Data Use Agreement.

The DPC Portal onboarding process provides a notice of PII that will be required to create an account.

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.

ACO and DPC APIs: Medicare beneficiaries may revoke access by contacting the 1-800 Medicare Call Center and requesting to changes to their data sharing preference.

DPC Portal: Providers and their delegates must undergo rigorous identity proofing to gain access, managed outside of the BCDA system leveraging Login.gov. Providers and their delegates are not

opted in by default, they may choose to not participate in the program.

AB2D API: This API does not have allow for opt out, as per the CMS Final Rule (84 FR 15680). The Final Rule specifies Part A and B data must be provided to PDPs, with no opt-out provisions. Substance Abuse and Mental Health (SAMHSA) claims data are not available to PDPs.

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

BCDA systems use information that is collected by other system applications. Those upstream system applications provide notices to the beneficiaries about any changes made to their data.

Any major changes that would affect the developers with CMS Credentials to the BCDA systems would be communicated through the established contact information they have provided, or through user and developer documentation published through developer.cms.gov as is appropriate for the change.

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.

Medicare beneficiaries may contact the 1-800 Medicare Call Center to resolve concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. Beneficiaries should be able to contact the business owner or system manager as stated in the System of Records Notice (SORN).

Providers and their delegates with DPC Portal accounts may contact dpcinfo@cms.hhs.gov with any concerns.

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

Every release deployment fully replaces the existing infrastructure and removes any transient data from the environment as part of the provisioning of the new environment where the application is running.

Claims data is stored in BFD. BCDA APIs cache and continually refresh this data from BFD.

Within the DPC Portal, Authorized Official PII is updated every time a Provider is linked to a new organization. Sources of current PII are Login.gov and PECOS.

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

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

Administrators of BCDA systems can access PII when assigned a specific role having that privilege. Roles are created using both the least privilege and need to know principles, so that no user has more access than they need. Administrator and support roles are designed to monitor and manage loading information and ensuring data consistency. Roles are reviewed at least annually to ensure that access to PII is still needed. BCDA systems are designed for external access through strict security controls that enable authenticated API clients to access beneficiary data in accordance with the entitlements granted to said API clients by virtue of their status as:

AB2D API: Authorized PDPs who have completed their attestation through the HPMS and the AB2D onboarding process. PDPs must use the data in accordance with the Federal Law and CMS Final

rule.

DPC API: vetted healthcare providers (e.g., providers in good standing with the National Plan and Provider Enumeration Systems)

ACO API: ACOs in good standing with ACO-OS. BCDA client owners realize the responsibility of safeguarding the PII or Protected health information (PHI) they house in their system.

Administrator and Support User roles are reviewed annually to ensure that access to PII is still needed.

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.

CMS staff and contractors may be required to review data in the system if questions are raised about how data is mapped to FHIR resources. In these cases, access to beneficiary information is tightly controlled and restricted to only the staff needed to perform the necessary validation of any data transformation process.

The environment that stores the beneficiary information is tightly controlled with multiple layers of protection. The architecture is multi-zoned as directed by CMS Policy. The ADO managing this environment has numerous controls in place to limit, monitor, and track individual access to the beneficiary data.

BCDA systems have been designed to automate software deployment. As an example, the software can be deployed to application servers via source-controlled scripts that enable machines to be built, configured, and deployed without requiring systems administration staff to connect to and manually configure the servers being deployed. This enables deployments to be closely tracked and avoids the need for administrators to access systems that may be handling PII/PHI.

Additionally, logs are captured in CMS-approved monitoring tools to be able to monitor access and detect anomalies. Other audit tasks include, but are not limited to, monitoring changes to user access privileges, and monitoring the identity and location of data access requests.

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.

Following the CMS security policy, BCDA management requires Security and Privacy Awareness Training for each user to maintain their access to the system. General users of the system are required to complete security awareness training to obtain a user account.

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

BCDA undergoes additional role-based training specific to the targeted roles of Program Managers, System Administrators, and Developers.

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.

We do not retain beneficiary records; once transmitted, the temporary data file is removed. AB2D API does cache some metadata (for example, MBIs) which is encrypted, and routinely destroyed and replaced with updated information from the BFD server.

For the DPC Portal, only standard account profiles related to Providers and their delegates are retained, including name and email address.

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

BCDA makes use of various controls and countermeasures to ensure that the confidentiality, integrity, and availability of the PII collected in the system remains secure. Some of those controls are listed below:

Architectural: BCDA APIs are split into two primary tiers, each having separate control systems. The BCDA front-end system exists within the CMS Cloud Services (CCS) environment and is implemented using the standards and components approved by CMS, such as a multi-zone architecture that separates different elements of the front-end platform.

The back-end data storage tier is built using the same CMS architectural standards for virtual Amazon Web Services (AWS) environments. Access control to the back-end API is limited using tightly controlled access certificates. All data communication is handled over secure links using Transport Layer Security (TLS) encrypted channels.

Administrative: Annual training is required for all administrators and staff regarding the handling of PII. Annual security assessment is conducted to ensure the correct controls are in place to protect the system and data collected. Continuous monitoring using automated tools is implemented.

Technical: BCDA utilizes multiple technical controls to protect PII records and prevent unauthorized access. Multi-Factor Authentication is enabled. API clients' primary means of accessing data is granted based on the validity of a credential known as an access token. Access tokens must be renewed on a regular basis. Data stored in the BCDA database and file system is also encrypted. In addition to preventative controls, BCDA audits key activities related to PII access within the system and centrally records them for ongoing monitoring and future retrieval:

Actions taken by BCDA staff members while administering the system are centrally recorded and archived for later inspection.

Actions taken by API clients -- both requests and responses.

Audit trail logs are retained by CMS in accordance with its security policies and requirements.

Physical: A smart card is needed to gain entrance to building and facilities. Government issued laptops and workstations are used and can only be accessed using authorized smart cards.

BCDA follows the data retention policy set forth by CMS regarding the type of data the system collects. Equipment and data are also sanitized and disposed of according to CMS and federal regulations.

Identify the publicly-available URL:

AB2D API Website
https://ab2d.cms.gov/

ACO API Website
https://bcda.cms.gov/

DPC API Website
https://dpc.cms.gov/

DPC Portal:
https://dpc.cms.gov/portal

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?

No

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.

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