US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/21/2026

OPDIV:

CMS

Name:

Blue Button API on Fast Healthcare Interoperability Resources

PIA Unique Identifier:

P-1048045-000365

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.

Alteration in Character of Data

New Public Access

New Interagency Uses

Internal Flow or Collection

Addition of IDR data to support required CMS Aligned Network for patient matching.

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

This is a CMS mandated change: Addition of IDR data (i.e SSN, Address, etc.) to support required CMS Aligned Network for patient matching.

Describe the purpose of the system.

Blue Button Application Programming Interface on Fast Healthcare Interoperability Resources (BBAPI) increases electronic access to health care information by giving Medicare beneficiaries the ability to connect their Medicare Part A, Part B, and Part D claims information to applications that they trust. The system also support patient matching allowing systems that register to be able to use

PII/PHI of a beneficiary to retrieve data through a matching process to support CMS Aligned Networks.

Applications, created by independent developers and not endorsed or certified by CMS, can be mobile applications, personal heath record platforms or research programs. These applications integrate with the BBAPI adding value for beneficiaries, providers, care organizations, and researchers to reduce patient burden, streamline information about different kinds of care over time, uncover new insights that can improve health outcomes, and the ability to access and monitor health information in one place.

The beneficiary's ability to see and receive their own health records is a legal right under the Health Insurance Portability and Accountability Act (HIPAA).

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

The claims data in the BBAPI is obtained from the following source systems which are covered under their own PIA: Medicare Integrated Data Repository (IDR), Chronic Condition Warehouse (CCW), Medicare Multi-Carrier Claims System (MCS), Fiscal Intermediary Shared System (FISS), Accountable Care Organization-Operational System (ACO-OS). ACO-OS data is transferred through the Beneficiary Fast Healthcare Interoperability Resources (FHIR) Data (BFD) system but not directly used in the system. The BFD application is included within the BBAPI FISMA system boundary and acts as the backend for the BBAPI. The BFD system transforms the data from the upstream systems in to a Fast Healthcare Interoperability Resources (FHIR) compliant data format.

Claims data maintained in the BBAPI includes explanation of benefits (EOB) for Part A, Part B and Part D claims data, pre-adjudicated claims, coverage data (i.e., Medicare plan type) and patient information that includes name, date of birth, sex, race, address, e-mail, phone numbers and deceased date. Provider information includes mailing address and tax number.

The Health Insurance Claim Number (HICN) and Medicare Beneficiary Identification (MBI) number are maintained and used for beneficiary matching. The Social Security Number (SSN) will also be used for beneficiary matching.

System access information on beneficiaries including details of the user, data accessed, and application authorization is maintained in the system.

BBAPI regularly uses PII to retrieve system records including using personal identifiers such as the name and user ID number of CMS employees and direct contractors authorized to control and authenticate access to the system.

Data is maintained (stored) in the system permanently.

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

BBAPI provides Fast Healthcare Interoperability Resources (FHIR)-formatted claims data for individual Medicare beneficiaries, to registered third-party applications with beneficiary authorization. (FHIR is a standard for exchanging healthcare information electronically).

A Medicare beneficiary chooses an application to connect their Medicare claims information. The application redirects the beneficiary to the BBAPI for authorization. The beneficiary verifies their identity using their MyMedicare.gov username and password (NOTE: username and password for MyMedicare.gov are not maintained by BBAPI). The patient identifier (i.e., HICN and MBI) is sent to the BBAPI for beneficiary matching. Provider's mailing address and tax number are also used for matching.

Token-based authentication is used to allow the application to verify their identity, and in return receive a unique access token. The application must supply this token on every request made to the BBAPI on behalf of the beneficiary.

Using the access token, the application makes a request to the BBAPI for the beneficiary data. BBAPI transmits the beneficiary data that includes, if applicable: explanation of benefits (EOB) for Part A, Part B and Part D claims data, coverage data (Medicare plan type) and patient information that includes name, date of birth, sex, race, address, e-mail, phone numbers, and deceased date to the application. The data is then made available to the beneficiary using the application.

BBAPI collects and maintains system access information on beneficiaries that include details of the user, data accessed and application authorization to validate every access made by an application to the BBAPI.

BBAPI regularly uses PII to retrieve system records including using personal identifiers such as the name and user ID number of CMS employees and direct contractors authorized to control and authenticate access to the system.

BBAPI regularly uses PII including using personal identifiers such as the hashes of the HICN and MBI to retrieve the claims data of Medicare beneficiaries.

BBAPI will also use asymmetric authentication with external partners such as Clear and ID.ME to allow 3rd party apps that have performed IAL2/AAL2 to make requests of the system using token based patient matching. This process will collect request data and use that data to validate against CMS data. If a match is successful an access token will be granted that will allow the 3rd party application to request all data related to that beneficiary within the system.

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
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Taxpayer ID
Date of Death, Therapy Records, Sex, Race, HICN, MBI, CMS credentials (name and user ID)

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

Employees
Public Citizens
Vendor/Suppliers/Contractors
Patients
Providers

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

BBAPI is designed for external access that enables an authenticated beneficiary to grant access to their PII to one or more applications of their choice. Access granted by a beneficiary releases their PII to the application.

BBAPI regularly uses PII to retrieve system records including using personal identifiers such as the name and user ID number of CMS employees and direct contractors authorized to control and authenticate access to the system including patient matching.

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

Testing and validation of expected operation and system behavior.

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

Sections 1902(a)(6), 1142(c)(6) of Title XVIII of the Social Security Act

Sections 1842, 1862 (b) and 1874 of Title XVIII of the Social Security Act (42 United States Code (U. S.C.) 1395u, 1395y (b), and 1395kk)

Sections 1816, 1862 (b) and 1874 of Title XVIII of the Social Security Act (42 U.S.C. 1395(h), 1395y (b), and 1395kk)

Section 723 of the Medicare Prescription Drug Improvement and Modernization Act of 2003 (Pub. L. 108-173)

Title IV of the Balanced Budget Act (Pub. L. 105-33).

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 Warehouse (CCW), 09-70-0501- Medicare Multi-Carrier Claims

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Other

Government Sources

Within the OpDiv

Non-Governmental Sources

Public

Commercial Data Broker

Private Sector

Identify the OMB information collection approval number and expiration date

Not Applicable.

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.

The Centers for Medicare & Medicaid Services approved Data Use Agreement.

Describe the procedures for accounting for disclosures.

The Data Use Agreement (DUA) is needed to ensure that the disclosure and use of Limited Data Sets derived from a CMS Privacy Act System of Records comply with 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).

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 claims data in the BBAPI is obtained from the following source systems which are covered under their own PIA: IDR, CCW, MCS, and FISS. ACO-OS data is transferred through the BFD system but not directly used in the system. Notice is the responsibility of the source 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.

The claims data in the BBAPI is obtained from the following source systems which are covered under their own PIA: IDR, CCW, MCS, FISS, and ACO-OS. These systems are responsible for providing methods for individuals to opt-out of collection or use of PII.

A Medicare beneficiary chooses an application to connect their Medicare claims information. The application redirects the beneficiary to the BBAPI for authorization. The beneficiary verifies their identity using their MyMedicare.gov username and password (NOTE: username and password for MyMedicare.gov are not collected by BBAPI). The beneficiary is provided with an authorization screen. Within the authorization screen, the beneficiary has the option to approve or decline authorization. If the beneficiary approves authorization, token-based authentication is used to allow the application to verify their identity, and in return receive a unique access token.

The application must supply this token on every API call (request) made to the BBAPI on behalf of the beneficiary. The application retains access to retrieve information for the beneficiary if the token remains valid. If a beneficiary revokes the authorization to their information, the token is invalidated, and the application will be unable to retrieve any information for the beneficiary.

Medicare beneficiaries can revoke the authorization by using these methods:

Beneficiaries can access their MyMedicare.gov account and revoke the authorization to the application.

Medicare Call Center agents can assist a beneficiary with revoking authorization to the application. Contact information: 1-800-MEDICARE (1-800-633-4227)

Beneficiaries can choose whether or not to share their personal information such as name, address, date of birth, race, and sex with the application. When the beneficiary reaches the authorization screen, radio buttons let a beneficiary select only one of two choices: share all your data or share healthcare data, but not personal info. The default selection is to share all data. If a beneficiary later decides they want to change their selection, they will need to repeat the authorization process.

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

The claims data in the BBAPI is obtained from the following source systems which are covered under their own PIA: IDR, CCW, MCS, FISS, and ACO-OS. These source systems are responsible for providing notices and obtaining consent when major changes occur to their systems.

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 claims data in the BBAPI is obtained from the following source systems which are covered under their own IDR, CCW, MCS, FISS, and ACO-OS

BBAPI system administrators can revoke application credentials for concerns that PII has been inappropriately obtained, used, or disclosed. This would prevent the application from using the BBAPI to access information for any beneficiary that provided an authorization.

If a beneficiary has concerns that their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate, they can use these methods for resolution:

Beneficiaries can access their MyMedicare.gov account and revoke the authorization to the application.

Beneficiaries can contact 1-800-MEDICARE (1-800-633-4227). Medicare call center agents have scripts available that can assist a beneficiary with a concern about an application that is connected to their information.

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

The claims data in the BBAPI is obtained from the following source systems which are covered under their own PIA: IDR, CCW, MCS, FISS, and ACO-OS. These source systems are responsible for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy, and relevancy.

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.

Access to PII is granted using the principles of least privilege and need to know; users are only granted access to PII based on their job responsibilities needed to perform their assigned duties. Role creation involves an analysis for the role definition and type of access.

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.

BBAPI system administrators, developers and direct contractors may be required to review PII maintained in the system to validate the mapping of data. In these instances, PII is restricted to only those users who are needed to perform the necessary validation.

The BBAPI platform is designed to automate software deployment. Software can be deployed to application servers by source-controlled scripts, without manual intervention, enabling deployments to be closely monitored and avoiding the need to access PII.

Security information and event management (SIEM) tools are used to monitor access and detect anomalies. Any anomalies are addressed and resolved by contacting the user, modifying their user access, or by removing their access if no longer required. Activities of all users including system administrators are logged and reviewed to identify abnormal activities.

The BB2.0 API grants access only to data at the beneficiary request to a specific onboarded application through medicare.gov Scalable Login Systems (SLS).

ACO-OS data is transferred through the BFD system but not directly used in the system.

For access through patient matching data is returned only if a successful match is made and only for the patient/beneficiary that is specifically matched.

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.

Security and privacy awareness training is provided to each user on an annual basis. All users are required to complete training to obtain a user account and annually thereafter.

Required training includes annual Department of Health and Human Services (HHS) Information Systems Security Awareness Training, annual HHS Privacy Training, reading, and attesting to the Rules of Behavior for Use of HHS Information Resources (HHS RoB)

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

Role-based training is required for those with significant information security and privacy responsibilities. BBAPI system administrators, developers and direct contractors are required to complete annual role-based training.

A sample list of role-based training includes Incident Response exercises, Contingency Planning exercises.

External systems though BB2.0 are made aware of the general privacy policy and are required to disclose their privacy policies.

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.

Records are maintained in accordance with the National Archives and Records Administration (NARA) records schedule: DM-0440-2015-0008. Records are retained for 7 years unless longer retention is authorized.

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

BBAPI implements multi-tier architecture, separating different components of the system into subnets. Each subnet is separated by a firewall that is configured to deny all traffic, unless explicitly allowed.

Administrative controls include annual security and privacy training for the proper handling of

information, configuration management, change management, periodic review of users, and deletion or revoking of user accounts.

Technical controls include multi-factor authentication, session locks, encryption, mutual transport layer security (TLS), firewalls, vulnerability scans, penetration testing, and monitoring.

Physical controls include a secure AWS data center, video surveillance, intrusion detection systems, uninterruptible power supply (UPS), back-up generators, environmental controls to maintain a constant operating temperature, smoke detection sensors, and sprinkler systems.

Identify the publicly-available URL:

https://bluebutton.cms.gov/

https://sandbox.bluebutton.cms.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.

Other technologies that do not collect PII:

Tealium and Adobe Analytics. This web analytics service is not being used to collect PII. Analytics is being used to determine how users are navigating through the BBAPI website and documentation to provide helpful insights that can be used to improve performance.

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?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null