US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/28/2018

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.

Test

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?

New

Does the system have Security Authorization (SA)?

No

Describe the purpose of the system.

Blue Button Application Programming Interface (BBAPI) on Fast Healthcare Interoperability Resources is a system that enables beneficiaries to connect their Medicare claims data to Third Party Applications (TPA). These TPAs may be Native Mobile Applications, Personal Health Record Platforms (e.g. Microsoft HealthVault) or Research Programs (e.g. the National Institute of Health's “All of Us” research initiative).

TPAs are developed by independent developers. These TPAs are not commissioned by or for CMS and are chosen by a Medicare beneficiary and used as part of their rights of access under the Health Insurance Portability and Accountability Act. These TPAs are typically acquired by a Medicare beneficiary from an external app store where their implementation is governed by the terms of those app stores (e.g. The iOS App or Google Play stores). These apps are outside of the CMS security boundary and therefore do not require a third party website application privacy impact assessment by CMS.

Medicare provides this information today through the BlueButton download feature on MyMedicare.gov that provides a PDF or text file download. The BBAPI delivers the data in a structured format that allows easier and more accurate processing with less effort required by the beneficiary.

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

The information in the BBAPI system includes the beneficiary name, address, birth date, gender, race and a randomly assigned beneficiary Identifier. It also includes an encrypted non-reversible hash of the Health Insurance Claim Number (HICN), which is only used for beneficiary matching. The coverage resource (a HL7 FHIR defined structured resource that BBAPI uses to express the Medicare Coverages that a Beneficiary holds) does not contain any PHI/PII. The coverage resource is linked by the arbitrary beneficiary ID to the patient resource. The explanation of benefit (EOB) resource does not contain any PII. It contains information about a claim. The EOB resource is linked by the arbitrary beneficiary ID.

Beneficiary user credentials are not stored by the BBAPI. Beneficiary authentication is handled by the MyMedicare.gov platform through a secure authentication API.

Developers of TPAs register with BBAPI in order to manage the security credentials and configuration information for the TPAs they want to connect to BBAPI. For those developers we store: Name, Email address, Organization (optional) and Mobile Phone (optional). These credentials are not shared with any other system. The email address is only used to enable account password resets.

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

The BBAPI manages four major elements: beneficiaries and their TPA authorizations, developers (of TPAs), applications (TPAs belonging to Developers), beneficiary claim information. Beneficiary authentication is handled by MyMedicare.gov via a secure channel.

Developers of TPAs register with BBAPI in order to manage the security credentials and configuration information for the TPAs they want to connect to BBAPI. For those developers we store: Name, Email address, Organization (optional) and Mobile Phone (optional).

Application information is maintained that enables BBAPI to communicate securely with the TPA. No PHI is stored for a TPA.

The beneficiary information (Patient, Coverage and EOB resources) is made available via a secure API to the beneficiary only when a beneficiary has specifically authorized a TPA to access and present their information. Each TPA has to be specifically authorized by the beneficiary and the details of the data accesses permitted, and the user and TPA authorization is stored in order to validate each and every access made by a TPA to the BBAPI.

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

Other: Per PIA-012 the Beneficiary’s Patient Resource will hold the following PII: Name, Address,

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

Providers

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The BBAPI has information about the beneficiary that enables a Medicare beneficiary to release their information to a TPA of their choosing. The beneficiary has control over which TPAs are able to receive their information.

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

Not applicable.

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

Section 1874(a) and 1875 of the Social Security Administration 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.

PECOS 09-70-0532, EDB 09-70-0502

NPS 09-70-008

NCH 09-70-0558

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

This system does not directly collect information from Medicare beneficiaries. The information in the BBAPI is from CMS' National Claims History (NCH) that is a subset of the CMS Chronic Conditions Warehouse (CCW) that is re-structured and used to effectuate a Medicare beneficiary's decision to allow an application to receive their information. The system that collects does collect information from a Medicare beneficiary has an OMB information collection approval number and expiration date.

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.

When a beneficiary uses a TPA that has registered with BBAPI they will click on a link that passes the beneficiary over from the TPA to the BBAPI. After successfully authenticating using their MyMedicare.gov user credentials they will be presented with an authorization screen. The beneficiary has the option to authorize or decline.

It is only if they click on the authorize button that a unique authorization token is returned to the TPA via a secure, pre-registered channel. The TPA must supply this token on every API call they make to BBAPI on behalf of the beneficiary. If they don’t use the token, or the beneficiary revokes the token, by visiting their account on MyMedicare.gov, the TPA will be unable to retrieve any data for the beneficiary.

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 beneficiary revokes access by contacting the BBAPI developer help desk that would use the administrative function to revoke their authorization.

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

The BBAPI system uses information that is collected by other system applications. Those system applications provide notices to the beneficiaries about any changes made to their data.

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.

If a beneficiary has concerns that they have authorized an inappropriate application to access their Medicare information via BBAPI they will have multiple avenues to resolve the issue:

They can access their MyMedicare.gov account and revoke the authorization to the TPA in question. They do not need to have access to the TPA itself in order to revoke access.

The 1-800 Medicare Call Center will have scripts to enable agents to assist a beneficiary with a concern about an application they have connected to their data.

If CMS has concerns about a particular TPA the protocol that is used to provide the beneficiary Authorization has a mechanism that allows CMS to revoke a TPA's credentials. This would prevent a TPA from using BBAPI to access information for any beneficiary that had provided them with an authorization token.

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 BBAPI administrators will conduct annual access reviews of user accounts to ensure that the users who have them still need them to carry out their daily job functions. This will also help identify users who have more access than they need, or need to have them removed. The goal of this review will also be to protect the PII contained in the system.

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

Administrators:

System administrators access data to manage system and troubleshoot potential issues.

Developers:

Developers access data in the process of managing and preparing data sets and data extracts.

Contractors:

Direct Contractors operating on behalf of the agency, using agency credentials are authorized by CMS to access data to conduct research under the assigned contract. Also, contract staff may assist in troubleshooting any issues that may arise.

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

Administrators of the BBAPI system are able to access PII as part of their job function and description. 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 information loading and ensuring data consistency. The BBAPI system owners realize the responsibility of safeguarding the PII or PHI it houses in its system. The BBAPI is designed for external access through a tightly controlled system of security controls that enable an authenticated Beneficiary to grant access to their data to one or more third party applications of their choice. Access granted by a Beneficiary to a Third-Party Application only grants access to the data belonging to that specific Beneficiary.

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 contractor managing this environment has numerous controls in place to limit, monitor, and track individual access to the beneficiary data.

The BBAPI platform has been designed to automate software deployment. As an example, 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.

In addition to this logs are captured in Splunk and other 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, the BBAPI 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).

BBAPI 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.

Records are maintained in accordance with the National Archives Records Schedule DAA-0440-2015-000-0001. Records are retained up to 10 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.

The BBAPI 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: The BBAPI platform is split into two primary environments. These each have separate control systems. The 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 environment is built using the same CMS architectural standards for virtual AWS environments and access control to the Back-end API is limited to only the Front-end Platform using tightly controlled access certificates. All data communication is handled over secure links using HTTPS/SSL encrypted channels.

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

Technical: Technical access control to records is provided by the system to prevent unauthorized users from viewing PII. Multi Factor Authentication is enabled as well to provide further security. Data in database is also encrypted, while VPN with TLS is used for data in transit. The system automatically logs a user off if they are inactive for a period of time.

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.

BBAPI 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:

https://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:

Google Analytics. This measurement service is not being used to collect PII. Google Analytics is used to develop statistics that help the BBAPI team to improve the flow of the application to make it easier for Beneficiaries to access their own claims information. Session customization technology is not used on the BBAPI.

Does the website have any information or pages directed at children under 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