Privacy Impact Assessment for the VA IT System called:

The Lighthouse Benefits (LHB) Application Programming interfaces (APIs)

Veteran Affairs Central Office (VACO)

Product Engineering Services

eMASS ID #2459

Date PIA submitted for review:

05/05/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	OITPrivacy@va.gov tonya.facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Yvonne Goudy-Bermudez	Yvonne.goudy-bermudez@va.gov	804-675-5000 x1017
Information System Owner	Jeremy Steinbeck	Jeremy.steinbeckr@va.gov	858-424-1294

Abstract

The abstract provides the simplest explanation for "what does the system do for VA?".

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) is a set of cloud-enabled Software as a Service (SaaS) services. The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) enable enhanced digital capabilities for interacting with the VA regarding Benefits Claims and Appeals process by providing an electronic means for participating in the Veterans Benefits Administration's claims and appeals processes. Capabilities include the searching and locating the latest versions of VA Forms, identifying acceptable values to be used for populating forms to decrease form errors, submitting digital forms by a Veteran or on a Veteran's behalf, submitting structured data used to auto-establish submissions, check the status for the form submissions, and manage personal banking information for receiving benefits payments via direct bank deposit. Providing these capabilities enables VA applications and/or approved third-party consumers to build applications which improve the speed, efficiency, accuracy, and overall Veteran or authorized Veteran representative experience while navigating the Veteran Benefits Administration claims and appeals processes.

Overview

The overview is the most important section of the Privacy Impact Assessment (PIA). A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) provides a set of the capabilities targeted at enabling VA and/or approved third-party consumers to build applications which improve the speed, efficiency, accuracy, and overall Veteran or authorized Veteran representative experience while navigating the Veteran Benefits Administration claims and appeals processes.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

VA Owned and Operated

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) will store claim, appeals, or other documents for approximately 1.8 million individuals. These are individuals (Veterans and non-Veteran claimants) who are submitting claims, appeals, or other

documents to the Veterans Business Administration for processing and review. The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) stores the information temporarily and no longer than 45 days past the date that the data has been accepted by the next system involved in the process. Additionally, names and VA email addresses of VA Employees and VA contractors working on the system are kept as records. This information is stored for the entire duration of their tenure working on the system.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☒	VA Employees
☐	Clinical Trainees
☒	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

D. What is a general description of the information in the IT system and the purpose for collecting this information?

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) collects the necessary information for the submission of the claims, appeals, or other documents to be further processed by VBA. The exact data is specific to the form that is being submitted but may include PII including name, social security number, date of birth, personal mailing address, personal telephone numbers, personal email address, financial information, health insurance beneficiary numbers, medical records, sex integrated control number, military history/service connection, benefits file number, and participant id. This information is collected in support of managing the claim, appeal, or document submission processes.

E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) enables enhanced digital interactions with VA systems for the purposes of establishing and processing claims and appeals and establishing accurate bank information for direct deposit to claimants. The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) accepts PII information related to claims, appeals and other documents and shares it with other VA systems which are required to complete the Veteran Benefits Administration establishment processes. These systems include Benefits Integration Services – Benefits Enterprise

Platform, Central Mail Portal, VBMS Claims Evidence, and Benefits Integration Platform (BIP). The PII information shared is required information for making submissions to the VA which may include name, social security number, date of birth, personal mailing address, personal telephone numbers, personal email address, financial information, health insurance beneficiary numbers, medical records, sex, integrated control number, military history/service connection, benefits file number, and participant id. Personal demographics and identifiers including name, social security number, date of birth, personal mailing address, personal telephone number, personal email address, sex, and integrated control number are used in conjunction with the Master Person Index to ensure that while sharing data between systems the information is being applied to the common claimant. The participant id is used to ensure that data shared with other VA systems is for a common claimant. Additionally, The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) will share status information, sourced from Caseflow, and direct deposit banking information, from Master Person Index and Benefits Integration Services, with authorized third-party commercial applications and authorized internal VA applications to provide current state information to claimants or their authorized representative for review and informational purposes. The third-party commercial applications are only allowed access to the information if it has been approved by the VA in an explicit information sharing agreement or if the individual or their authorized representative has provided direct consent to the application using OAuth2.

F. Are the modules/subsystems only applicable if information is shared?

Yes

G. Is the system operated in more than one site to include primary and secondary site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) is hosted in the VA-controlled Cloud Computing Environment, Veterans Affairs Enterprise Cloud (VAEC) Amazon Web Services (AWS). The system and data reside in the VAEC AWS GovCloud environment.

3. Legal Authority and System of Record Notices (SORN)

H. What is the citation of the legal authority?

- Title 10 U.S.C. chapters 106a, 510, 1606 and 1607
- Title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32,33, 34, 35, 36, 37, 39, 51, 53, 55 and 77
- Title 5 U.S.C 5514
- Title 38 United States Code 5701
- The Privacy Act of 1974, 5 U.S.C § 552a
- Title 38 of the United States Code, Sections 501(a)
- Title 38 of the United States Code, Sections 501(b) and 304
- 38 U.S.C. 501

I. What is the SORN?

- Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA-VA (58VA21/22/28 / 86 FR 61858) 58VA21/22/28 / 86 FR 61858
- Veterans Appellate Records System-VA (44VA01/ 88 FR 44185) 44VA01/ 88 FR44185
- Patient Medical Records-VA (24VA10A7 / 85 FR 62406) 24VA10A7 / 85 FR 62406
- National Patient Databases-VA (121VA10 / 88 FR 22112) 121VA10 / 88 FR 22112
- Veterans Health Information Systems and Technology Architecture (VistA) Records –VA 79VA10 / 85 FR 84114
- Department of Veterans Affairs Identity Management System (VAIDMS) 146VA0005Q3 / 73 FR 16093

J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

SORNs applicable to The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) do not require amendment or revision or approval. All applicable SORNs cover cloud usage and storage.

4. System Changes

K. Will the business processes change due to the information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

I. Will the technology changes impact information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 Information collected, used, disseminated, created, or maintained in the system.

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority to Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ **Full** Social Security Number
- ☐ **Partial** Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a Different Individual)
- ☒ Financial Information
- ☒ Health Insurance Beneficiary Numbers Account Numbers
- ☐ Certificate/License Numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☒ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Sex
- ☒ Integrated Control Number (ICN)
- ☒ Military History/Service Connection
- ☐ Next of Kin
- ☐ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal Identifier (EDIPI)
- ☒ Other Data Elements (List Below)

Other PII/PHI data elements:

- Benefits File Number
- Participant ID

1.2 List the sources of the information in the system
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) enables enhanced digital interactions with VA systems for the purposes of establishing and processing claims and appeals and establishing accurate bank information for direct deposit to claimants. The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) accepts PII information related to claims, appeals and other documents and shares it with other VA systems which are required to complete the Veteran Benefits Administration establishment processes. These systems include Benefits Integration Services – Benefits Enterprise Platform, Central Mail Portal, VBMS Claims Evidence, and Benefits Integration Platform. The PII information shared is required information for making submissions to the VA which may include name, social security number, date of birth, personal mailing address, personal telephone numbers, personal email address, financial information, health insurance beneficiary numbers, medical records, sex, integrated control number, military history/service connection, benefits file number, and participant id. Personal demographics and identifiers including name, social security number, date of birth, personal mailing address, personal telephone number, personal email address, sex, and integrated control number are used in conjunction with the Master Person Index to ensure that while sharing data between systems the information is being applied to the common claimant. The participant id is used to ensure that data shared with other VA systems is for a common claimant. Additionally, The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) will share status information, sourced from Caseflow, and direct deposit banking information, from Master Person Index and Benefits Integration Services, with authorized third-party commercial applications and authorized internal VA applications to provide current state information to claimants or their authorized representative for review and informational purposes. The third-party commercial applications are only allowed access to the information if it has been approved by the VA in an explicit information sharing agreement or if the individual or their authorized representative has provided direct consent to the application using OAuth2.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) enable machine to machine communication of the information allowing for more applications to be developed that interface directly with individuals or their authorized representatives in the VA Benefits processes. Additionally, The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) provide data to these authorized applications to support keeping the individual or their authorized representative informed of the current state of processing within the VA processes.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

Yes, The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) can create claims, appeals, and other document forms given the provided information from the authorized caller of the APIs and information gathered from VA sources Benefits Integration Services and the Master

Person Index for the forms being supported. These generated forms are sent to other systems in the VA such as Benefits Integration Services, Central Mail Portal or VBMS Claims Evidence for further processing.

1.3 Methods of information collection

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) receives and transmits all information electronically. Information is received from authorized third-party applications and authorized internal VA applications via RESTful APIs using JSON/https and binary documents. Interactions with Benefits Integration Service and Master Person Index are accomplished using SOAP APIs. Interactions with Central Mail Portal, Caseflow, and Benefits Integration Platform use JSON/https. Interactions with VBMS Claims Evidence are through direct TCP connections. Information processed is safeguarded in accordance with VA Handbook 6500, FIPS 140-2 encryption, and data processing standards.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

The information collected is to facilitate the submission of existing approved VA forms and is not subject to the Paperwork Reduction Act.

1.4 Information checks for accuracy, and how often will it be checked.

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Generally, The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) does not check data for accuracy. The integrity of the data is the responsibility of the data source either the other internal VA system or the application providing the information. Claims, Appeals, and other supporting documents are submitted to the next steps of the process which involve their own reviews for accuracy. When information is submitted for a claimant by an authorized representative (Power of Attorney), The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) will verify the representative responsible for the submission is the Power of Attorney on record for the claimant using the Master Patient Index.

Data in transit is protected using standards in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data at rest is encrypted using AWS Key Management System.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) checks every submission made by a representative that they are the representative of record for the claimant in the Master Person Index.

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA-VA (58VA21/22/28 / 86 FR 61858) 58VA21/22/28 / 86 FR 61858

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
Title 10 U.S.C. chapters 106a, 510, 1606 and 1607
Title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77.
Title 5 U.S.C. 5514

Veterans Appellate Records System-VA (44VA01/ 78 FR 66803) 44VA01/ 78 FR 66803

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
Title 38 United States Code 5701
The Privacy Act of 1974, 5 U.S.C. § 552a.
Title 38 of the United States Code, Sections 501(a))

Patient Medical Records-VA (24VA10A7 / 85 FR 62406) 24VA10A7 / 85 FR 62406

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
Title 38, United States Code, Sections 501(b) and 304

National Patient Databases-VA (121VA10 / 88 FR 22112) 121VA10 / 88 FR 22112

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
38 U.S.C 501

Veterans Health Information Systems and Technology Architecture (VistA) Records –VA 79VA10 / 85 FR 84114

Department of Veterans Affairs Identity Management System (VAIDMS) 146VA0005Q3 /73 FR 16093

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) processes Personally Identifiable Information which can be used to identify a Veteran or individual. If this information is breached or disclosed inappropriately then this could result in personal or financial harm to the individual whose information was exposed and provide a negative impact to the VA.

Mitigation: The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) protects data at rest using AWS standards and data in transit is protecting using standards in accordance with VA Handbook 6500 and FIPS 140-2. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted by the VA Project Manager and System Owner. VA Annual privacy and security training compliance will be enforced for VA Employees, contractors, and vendors. The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) use OAuth 2.0 enabling implementation of the Principle of Least Privilege for granting access to endpoints and data.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	Internal Use	External Use
Name	Identity validation, Used for digital benefit form submissions into the VA system(s) of record ("Benefit Submissions"), Used to retrieve, modify, or add benefit	Not used

	details to VA system(s) of record ("Benefits Management");	
Social Security Number	Identity validation, Benefit Submissions, Benefits Management	Not used
Date of Birth	Benefits Submissions	Not used
Personal Mailing Address	Benefits Submissions, Benefits Management	Not used
Personal Phone Number (s)	Benefits Submissions, Benefits Management	Not used
Personal Email Address	Benefit Submissions, used to send email notifications to veterans about their submission progress.	Not used
Financial Information	Uses bank routing and account information to update direct deposit information for receiving benefits payments, Benefits Management	Not used
Health Insurance Beneficiary Numbers	Benefits Submission, Identity validation	Not used
Medical Records	Used as evidence records to submit alongside Benefit Submissions, Used to directly submit documents to VA system(s) of record	Not used
Integrated Control Number (ICN)	Identity validation, internal recordkeeping, Benefit Submission, Benefits Management	Not used
Military History/Service Connection	Benefit submissions, Benefits Management	Not used
Benefits File Number	Benefit submissions, Benefits Management	Not used
Participant ID	Benefit Submission, Benefits Management	Not used

2.2 Describe the types of tools used to analyze data and what type of data may be produced.
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) does not create any data from analysis. It processes the information provided to the extent that is necessary to progress information to the next stage of processing within the VA.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) gets data from authorized application consumers and other VA systems to generate the completed copies of Veterans Benefits Administration forms and other documents. These documents are then submitted for processing to become part of the individual’s record. New records may be created by VA using this information if necessary to maintain the records of newly eligible claimants (usually, individuals with no prior record will be non-Veteran claimants). Actions may then be taken by Government employees within VA who use the information provided by claimants to determine the claimant’s eligibility for benefits, claims which may be approved, partially or in whole, or denied.

2.3 How the information in the system is secured.
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

Data is encrypted in transit (TLS 1.2+) and uses authenticated access (i.e API Keys, OAuth 2.0 access tokens). Data at rest is encrypted within AWS using AES-256.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

No additional SSN protections are in place beyond being encrypted in transit and being encrypted at rest.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) runs entirely in the VAEC AWS cloud satisfying the requirements of OMB Memorandum M-06-15

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) grants access using the principle of least privilege, only granting access to the data request by the consumer, consented by the individual or their authorized representative and approved by the System owner. The individual or their authorized representative requesting access to the data via an application must be provided the ability to revoke consent at any time. Other applications accessing data must have an explicit data sharing agreement with the VA (e.g. ISA/MOU, CRADA). API credentials are only issued upon System Owner approval.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Security controls are in place to ensure data is used and protected in accordance with legal requirements, VA cyber security policies, and VA's stated purpose for using the data. Audits are performed to verify information is accessed and retrieved appropriately. The following implemented Privacy Controls are in accordance with NIST SP 800-53-rev-4 Rules of Behavior, Two Factor Authentication, VA Privacy and Security Training, VA Safeguard and Awareness Training.

2.4c Does access require manager approval?

Yes, System Owner approval is required for access.

2.4d Is access to the PII being monitored, tracked, or recorded?

Yes

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

System Owner

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

Data related to the submission of benefits claims, appeals, or other supporting documentation is retained in temporary storage. This includes any PII that are part of the submission such as name, social security number, date of birth, personal mailing address, personal telephone numbers, personal email address, financial information, health insurance beneficiary numbers, medical records, sex, integrated control number, military history/service connection, benefits file number, and participant id.

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods**.** If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

Data is retained in temporary storage no longer than 45 days past the date that the submission of the benefit claim, appeal, or other supporting documentation has been confirmed received by the next VA system in the process.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. Please work with the system VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes

3.3b Please indicate each records retention schedule, series, and disposition authority?

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) adheres to VHA Records Control Schedule (RCS) 10-1 6000.1d (N1-15-91-6 item 1d) and 6000.2b (N1-15-02-3 item 3) which are approved by the VA records office and NARA and is indicated in the federal register. It is the main authority for the retention and disposition requirements of VHA records. It provides a brief description of the records and states the retention period and disposition requirements. It also provides the NARA disposition authorities or the GRS authorities, whichever is appropriate for the records, in addition to program and service sections.

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) also adheres to Records Control Schedule VB-1, Part 1 Section XIII, Item 13-052.100 as indicated in the federal register and authorized by NARA.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated, or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

The temporary storage of information related to claims, appeals or other document submission is electronic only and the files and data are deleted from the encrypted data store running within AWS.

The Lighthouse Benefits (LHB) Application Programming Interfaces adheres to VA Directive 6500 VA Cybersecurity Program

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training, and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) do not use any of the information for Testing, Training, or research purposes.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document in this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe policies and procedures for how PII that is no longer relevant and necessary is purged.
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) processes Personally Identifiable Information which can be used to identify a Veteran or individual. If this information is breached or disclosed inappropriately then this could result in personal or financial harm to the individual whose information was exposed and provide a negative impact to the VA

Mitigation: The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) protects data at rest using AWS standards and data in transit is protecting using standards in accordance with VA Handbook 6500 and FIPs 140-2. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted by the VA Project Manager and System Owner. VA Annual privacy and security training compliance will be enforced for VA Employees, contractors, and vendors. The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) use OAuth 2.0 enabling implementation of the Principle of Least Privilege for granting access to endpoints and data.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

PII Mapping of Components

4.1a The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) consists of eleven key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
Appeals Status API	Yes	No	Social Security Number Integrated Control Number (ICN)	Used to identify the individual about whom the information is being requested.	The data is used transiently in a single transaction and is not stored. Data in transit is protected using encryption in accordance

					with FIPS 140-2
Benefits Claims API	Yes	Yes	Name Social Security Number Date of Birth Personal Mailing Address Personal Telephone Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers/Account Numbers Medical Records Integrated Control Number (ICN) Military History / Service Connection Benefits File Number Participant ID	This includes the data necessary for generating the desired Benefits Claim with the VA	Data is held only long enough to ensure it has been successfully transferred to the next system. Data at rest is encrypted using the AWS Key Management Service. Data in transit is protected using encryption in accordance with FIPS 140-2
Benefits Documents API	Yes	Yes	Name Social Security Number Personal Mailing Address Personal Telephone Number Personal Email Address Medical Records Integrated Control Number (ICN) Benefits File Number Participant ID	To allow claimants to submit the information to the VA and continue to work on their behalf after initial submission to ensure further processing.	Data is held no longer than 45 days past the date it has been successfully transferred to the next system. Data at rest is encrypted using the AWS Key Management Service.

					Data in transit is protected using encryption in accordance with FIPS 140-2
Benefits Intake API	Yes	Yes	Name Social Security Number Medical Records Integrated Control Number (ICN) Benefits File Number	To allow claimants to submit the information to the VA and continue to work on their behalf after initial submission to ensure further processing.	Data is held no longer than 45 days past the date it has been successfully transferred to the next system. Data at rest is encrypted using the AWS Key Management Service. Data in transit is protected using encryption in accordance with FIPS 140-2
Decision Reviews API	Yes	Yes	Name Social Security Number Date of Birth Personal Mailing Address Personal Telephone Number Personal Email Address Health Insurance Beneficiary Numbers / Account Numbers Medical Records	To provide and manage benefits for Veterans and Non-Veteran Claimants	Data is held no longer than 45 days past the date it has been successfully transferred to the next system. Data at rest is encrypted using the AWS Key Management Service.

			Integrated Control Number (ICN) Benefits File Number		Data in transit is protected using encryption in accordance with FIPS 140-2
Direct Deposit Management API	Yes	No	Financial Information Integrated Control Number (ICN)	To allow claimants to manage their direct deposit bank information on file with the VA for receiving benefits payments.	The data is used transiently in a single transaction and is not stored. Data in transit is protected using encryption in accordance with FIPS 140-2
Appealable Issues API	Yes	No	Medical Records Integrated Control Number (ICN)	To provide and manage benefits for Veterans and Non-Veteran Claimants	The data is used transiently in a single transaction and is not stored. Data in transit is protected using encryption in accordance with FIPS 140-2
Legacy Appeals API	Yes	No	Name Medical Records Integrated Control Number (ICN)	To provide and manage benefits for Veterans and Non-Veteran Claimants	The data is used transiently in a single transaction and is not stored. Data in transit is

					protected using encryption in accordance with FIPS 140-2
Higher Level Reviews API	Yes	Yes	Name Social Security Number Date of Birth Personal Mailing Address Personal Telephone Number Personal Email Address Health Insurance Beneficiary Numbers / Account Numbers Medical Records Integrated Control Number (ICN) Benefits File Number	To provide and manage benefits for Veterans and Non-Veteran Claimants	Data is held no longer than 45 days past the date it has been successfully transferred to the next system. Data at rest is encrypted using the AWS Key Management Service. Data in transit is protected using encryption in accordance with FIPS 140-2
Notice Of Disagreement API	Yes	Yes	Name Social Security Number Date of Birth Personal Mailing Address Personal Telephone Number Personal Email Address Health Insurance Beneficiary Numbers / Account Numbers Medical Records Integrated Control Number (ICN)	To provide and manage benefits for Veterans and Non-Veteran Claimants	Data is held no longer than 45 days past the date it has been successfully transferred to the next system. Data at rest is encrypted using the AWS Key Management Service. Data in transit is protected using

			Benefits File Number		encryption in accordance with FIPS 140-2
Supplemental Claims API	Yes	Yes	Name Social Security Number Date of Birth Personal Mailing Address Personal Telephone Number Personal Email Address Health Insurance Beneficiary Numbers / Account Numbers Medical Records Integrated Control Number (ICN) Benefits File Number	To provide and manage benefits for Veterans and Non-Veteran Claimants	Data is held no longer than 45 days past the date it has been successfully transferred to the next system. Data at rest is encrypted using the AWS Key Management Service. Data in transit is protected using encryption in accordance with FIPS 140-2

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Veteran Benefits Administration (VBA) Benefits Gateway Services – Benefits Enterprise Platform	To provide and manage benefits for Veterans and Non-veteran claimants	Name Social Security Number Date of Birth Personal Mailing Address Personal Telephone Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers / Account Numbers Integrated Control Number (ICN) Benefits File Number	Hypertext Transfer Protocol – Secure (HTTPS)
Board of Veterans Appeals (BVA) Caseflow	To gather a veteran's appeal status, appealable issues, and legacy appeal data	Social Security Number Medical Records Integrated Control Number (ICN)	HTTPS
Veteran Benefits Administration (VBA) Central Mail Portal	Upload files & metadata to intake specialists for processing.	Name Social Security Number Personal Mailing Address Personal Telephone Number Personal Email Address Health Insurance Beneficiary Numbers / Account Numbers Medical Records Integrated Control Number (ICN) Benefits File Number	HTTPS
Veteran Benefits Administration (VBA) VBMS Claims Evidence	Establishing evidentiary documents for claims processing	Medical Records Benefits File Number Participant ID	HTTPS
Office of Information and Technology (OI&T) Master Person Index	Retrieve more veteran information from available on-record data.	Name Social Security Number Date of Birth Personal Mailing Address	HTTPS

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		Personal Telephone Number Personal Email Address Integrated Control Number (ICN) Participant ID	
Veteran Experience Office (VEO) VA Notify – Va.gov Veteran Facing Services Platform	Sending benefits status emails to veterans or non-veteran claimants.	Name Personal Email Address	HTTPS
Veteran Benefits Administration (VBA) Veteran Benefits Management System (VBMS)	Establishing forms and evidentiary documents for claims processing, retrieving benefits document statuses.	Integrated Control Number (ICN) Benefits File Number Participant ID	HTTPS
Office of Information and Technology (OI&T) Digital Veterans Platform	Digital Veterans Platform controls the API Gateway through which incoming traffic passes to reach the The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs)	Name Social Security Number Date of Birth Personal Mailing Address Personal Telephone Number Personal Email Address Financial Information Medical Records Integrated Control Number (ICN) Military History / Service Connection Benefits File Number Health Insurance Beneficiary Numbers / Account Numbers Participant ID	HTTPS
Veteran Benefits Administration (VBA) Benefits Integration Platform	Correlate Benefits Claims information across VA systems ensuring that Benefits Documents are being associated to the correct person and claims.	Name Participant ID	HTTPS

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

Discuss the privacy risks associated with the sharing of information within the VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) processes Personally Identifiable Information which can be used to identify a Veteran or individual. If this information is breached or disclosed inappropriately then this could result in personal or financial harm to the individual whose information was exposed and provide a negative impact to the VA.

Mitigation: The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) protects data in transit is protecting using standards in accordance with VA Handbook 6500 and FIPs 140-2. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted by the VA Project Manager and System Owner. VA Annual privacy and security training compliance will be enforced for VA Employees, contractors, and vendors. The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) use OAuth 2.0 enabling implementation of the Principle of Least Privilege for granting access to endpoints and data.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a

Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) does not provide external sharing.

Mitigation: The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) does not provide external sharing.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

Notice is provided as part of the Privacy Policy of the applications consuming the APIs and through either direct consent with the individual or authorized representative or via an explicit data sharing agreement such an ISA/MOU or CRADA which can be made available.

This Privacy Assessment (PIA) serves as notice. As required by the eGovernment Act of 2002, Pub.L.107—347 208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agencies. VA system of record notices (SORNs) are published in the Federal Register and are available online.

- Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA-VA (58VA21/22/28 / 86 FR 61858) 58VA21/22/28 /86 FR 61858
- Veterans Appellate Records System-VA (44VA01/ 88 FR 44185) 44VA01/ 88 FR44185
- Patient Medical Records-VA (24VA10A7 / 85 FR 62406) 24VA10A7 / 85 FR62406
- National Patient Databases-VA (121VA10 / 88 FR 22112) 121VA10 / 88 FR22112
- Veterans Health Information Systems and Technology Architecture (VistA)Records – VA 79VA10 / 85 FR 84114
- Department of Veterans Affairs Identity Management System (VAIDMS)146VA0005Q3 / 73 FR 16093

Additionally, each form supported by the APIs includes a Privacy Act Notice.

6.1b If notice was not provided, explain why.

Notice is provided

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

The privacy policies and notices were drafted and published by VA and list the privacy rights of claimants under the Privacy Act of 1974, and various elements of Title 38 of US Code

(specifically, 38 USC 3471, 5101, and 5701), and the rights for VA to use and disclose the information provided by claimants as necessary.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Yes, individuals can decline to provide information. In this case, they are unable to use applications that use The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) for the submission of information to the VA because the data they are sharing is what is necessary for the claims, appeals, or document submission.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

The information is only accessed when the process is initiated by an individual. If an individual does not engage with an application which uses The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) then there will be no information in The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) for sharing.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

<u>Principle of Transparency:</u> This is referring to sufficient notice provided to the individual.

<u>Principle of Use Limitation:</u> The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must ensure that information is used only for the purpose articulated in the notice.
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.

Follow the format below:

Privacy Risk: There is risk that individuals will not know the extent of information gathered in support of claims and appeals submissions.

Mitigation: The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) mitigates this risk by providing this PIA as notice of information processing.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 The procedures that allow individuals to gain access to their information.

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) transmit data supplied by claimants or their accredited representatives to VA systems, including VBMS and Caseflow. To request access to their data, an individual can file a proper Freedom of Information Act (FOIA) request with VA, which is detailed on https://department.va.gov/foia/. Accredited representatives who use software that rely on The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs), are entitled to access to VBMS. Claimants may also check with their accredited representative and ask about the accuracy of their information within VA systems. If claimants want a copy of their eFolder/cFile, this must still be requested via FOIA. Accredited representatives do not print copies for claimants, despite their access to VBMS. If the claimant or their accredited representative identifies incorrect information, this can be corrected by submitting the correction and supporting evidence, if required, to VA. Corrections may be submitted digitally, mailed, sent by fax, or some may be submitted over the phone by calling. 800-698-2411 Information on what is required to change specific types of information is identified in the M21-1 Adjudication Manual.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) is not exempt from the Privacy Act

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) is a Privacy Act system.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

If the claimant or their accredited representative identifies incorrect information, this can be corrected by submitting the correction and supporting evidence, if required, to VA. Corrections may be submitted digitally, mailed, sent by fax, or some may be submitted over the phone by calling. 800-698-2411. Information on what is required to change specific types of information is identified in the M21-1 Adjudication Manual.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) route information provided by claimants or their accredited representatives to VA systems, including VBMS and Caseflow. The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) do not keep data in a state that would be viewable or correctable by claimants or their representatives. Claimants are made aware of the procedures to correct their data in VA systems is detailed in the Resources and Support section of the va.gov website.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

If the claimant or their accredited representative identifies incorrect information, this can be corrected by submitting the correction and supporting evidence, if required, to VA. Corrections may be submitted digitally, mailed, sent by fax, or some may be submitted over the phone by calling 800-

698-2411. Information on what is required to change specific types of information is identified in the M21-1 Adjudication Manual

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) route information provided by claimants or their accredited representatives to VA systems, including VBMS and Caseflow. The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) do not keep data in a state that would be viewable or correctable by claimants or their representatives. Claimants are made aware of the procedures to correct their data in VA systems is detailed in the Resources and Support section of the va.gov website.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

Principle of Individual Participation: If access and/or correction is denied, then is the individual must be provided notice as to why the denial was made and how to challenge such a denial.

Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that inaccuracies in the data held and used by VA may cause incidental and unintended disclosures of private information (e.g. notification letters might be sent to a claimant's old address). Additionally, there is a risk that individuals not party to information held by VA in the various systems used during its activities may gain access to it or abuse redress and correction procedures to alter it.

Mitigation: Claimants or their accredited representative may review information for accuracy by accessing it directly in claimant's VA.gov profile, in VBMS, or via FOIA and may request VA correct any information they identify as inaccurate. It's outside the purview of The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) to determine the accuracy and validity of those requests since it routes the information to other VA systems like Caseflow and VBMS. Redress and correction procedures are handled and protected by VA and the policies of the systems which store the information. Access through The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) is enforced by strict authorization procedures. API consumer connections are encrypted in transit and agree to the VA API Terms of Service (ToS) / Code of Conduct (CoC) while also submitting to an approval process involving the System Owner. Access

controls are in place as dictated by VA's Risk Management Framework process, following required VA Handbook 6500 and NIST Guidelines. Audit log information is forwarded to the Cybersecurity Operations Center (CSOC) for continuous review and monitoring via installed agents by the VA Enterprise Cloud. The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) has continuous monitoring and alerting in place to detect traffic anomalies and malicious attempts to gain unauthorized access.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

An individual is onboarded as a The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) team member. Accounts are approved by the System Owner before they are created. Once approved, Lighthouse adheres to project roles maintained by the VAEC mapped back to VA Active Directory groups (e.g. read-only user, project admin, etc.) depending on the employee's role.

Any consumers of the system must be approved by the System Owner before access is granted.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Users from other agencies do not have direct access to The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs).

Other agencies can become consumer of the APIs provided of The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs). In this event these applications developed by other government agencies must be granted explicit consent by the individual or authorized representative or have and established data sharing agreement with the VA Privacy Office.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

An individual is onboarded as a The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) team member. Accounts are approved by the System Owner before they are created. Once approved, Lighthouse adheres to project roles maintained by the VAEC mapped back to VA Active Directory groups (e.g. read-only user, project admin, etc.) depending on the employee's role.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

How frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

VA Privacy and Information Security Awareness Rules Behavior is signed annually.

8.2a. Will VA contractors have access to the system and the PII?

Yes

8.2b. What involvement will contractors have with the design and maintenance of the system?

Contractors are primarily responsible for the design and maintenance of the system.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

VA Privacy and Security Training, VA Safeguard and Awareness Training, Privacy and HIPAA Training

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

1. *The Security Plan Status:* **Approved, 30/Oct/2023**
2. *The System Security Plan Status Date:* **3/Mar/2025**
3. *The Authorization Status:* **Authorization To Operate (ATO)**
4. *The Authorization Date:* **7/Aug/2024**
5. *The Authorization Termination Date:* **Ongoing until rescinded by Authorizing Official (AO)**
6. *The Risk Review Completion Date:* **5/Mar/2025**
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* **Moderate**

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

Completed

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

Yes VAEC AWS GovCloud Environment Software as a Service (SaaS)

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.1 of the PTA)* *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

All data is owned by the VA.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.

The cloud service provider does not collect any ancillary data.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The system owners and the contractors designing and maintaining the system are responsible for protecting the data contained therein or passing through. The cloud provider may hold logs of calls made to the system.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

The Lighthouse Benefits (LHB) Application Programming Interfaces (APIs) system does not use Robotic Process Automation.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research

ID	Privacy Controls
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

TONYA FACEMIRE

Digitally signed by TONYA FACEMIRE
Date: 2025.05.14 15:38:46 -04'00'

Privacy Officer, Tonya Facemire

YVONNE GOUDY-BERMUDEZ

Digitally signed by YVONNE GOUDY-BERMUDEZ
Date: 2025.05.13 13:40:28 -04'00'

Information Systems Security Officer, Yvonne Goudy-Bermudez

JEREMY STEINBECK

Digitally signed by JEREMY STEINBECK
Date: 2025.05.13 10:20:32 -07'00'

Information Systems Owner, Jeremy Steinbeck

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

Privacy Act Notice on Form - 526ez
Privacy Act Notice on Form - 21-22a

Privacy Act Notice on Form - 20-0995

Privacy Act Notice on Form – 20-0996

Privacy Act Notice on Form - 10182

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)