



Privacy Impact Assessment for the VA IT System called:

Salesforce - VA Lighthouse API Support

Veteran Affairs Central Office

Office of Information Technology Project Special Forces

eMASS ID #:1951

Date PIA submitted for review:

11/26/2024

System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	Gina.siefert@va.gov oitprivacy@va.gov	202-632-8430
Information System Security Officer (ISSO)	James Boring	James.Borning@va.gov	215-842-2000 x4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

The abstract provides the simplest explanation for “what does the system do?”.

This system is used for tracking support requests for the VA Lighthouse Application Programming Interface (API) program. It is a customer relationship management and ticket tracking system (Salesforce Service Cloud). Email correspondence for each case is retained, and the system tracks metrics on the volume and frequency of support requests.

Overview

The overview is the most important section of the 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?

This system is used for tracking support requests for the VA Lighthouse Application Programming Interface (API) program. It is a customer relationship management and ticket tracking system (Salesforce Service Cloud). Email correspondence for each case is retained, and this aids in tracking metrics on the volume, type, and frequency of support requests received. Lighthouse is a public API platform which supports external developers, who aren't under a contract with the VA, to develop applications for the VA. These developers, who are outside of the VA, have no VA email address.

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.

Lighthouse Public API Platform Product Owner and Director / Lighthouse Program Lead

2. Information Collection and Sharing

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

The current number of individuals whose information is stored in the system is around 3,000. The typical client or affected individual is a third-party developer, account executive, product/product manager, or student.

Check if Applicable	Demographic of individuals
<input checked="" type="checkbox"/>	Veterans or Dependents
<input type="checkbox"/>	VA Employees
<input type="checkbox"/>	Clinical Trainees
<input checked="" type="checkbox"/>	VA Contractors
<input checked="" type="checkbox"/>	Members of the Public/Individuals
<input type="checkbox"/>	Volunteers

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

Basic demographic information (First Name, Last Name, Email address, etc.) is collected to link users to the appropriate contact support history and notify users of upcoming changes/maintenance windows.

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

Users share and submit information through sandbox access requests, production access requests, or developer support requests.

Users submit information to obtain access to APIs via **sandbox access requests** on developer.va.gov. This data is stored in Lighthouse Platform Backend (“LPB”) within the Digital Veterans Platform (DVP) ATO boundary. Subsequently, data is manually inputted into Salesforce for case and account creation by an internal VA API support team.

When users sign up for **access to Lighthouse APIs in production environments** or **request API support** via the Developer Portal Support form on developer.va.gov, this data is stored in LPB within the DVP ATO boundary. LPB generates a mailer with stored metadata and sends it to api@va.gov. The incoming email from vets.gov@public.govdelivery.com creates a Case in Salesforce via the email-to-case workflow. Using an API endpoint from LPB, Salesforce ingests raw signup data periodically (i.e., GET requests retrieve any new API access/signup requests for a specified time range).

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

Yes.

G. Is the system operated in more than one 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 system is operated on one site.

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

H. What is the citation of the legal authority and SORN to operate the IT system?

As per the SORN, the authority for maintaining this system is Title 38 U.S.C. 5106.

H. What is the SORN?

The relevant SORN applicable for the system is “Case and Correspondence Management (CCM)–VA (75VA001B). The SORN covers all Personally Identifiable Information (PII) used in Salesforce - VA Lighthouse API Support.

I. SORN revisions/modification

This SORN does not require a revision and/or modification.

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

The system is in the process of being modified, however the SORN will not require amendment or revision and approval.

4. System Changes

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

Yes

No

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

Yes

No

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 What information is 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:

- | | | |
|---|---|--|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Financial Information | <input type="checkbox"/> Gender/Sex |
| <input type="checkbox"/> Full Social Security Number | <input type="checkbox"/> Health Insurance Beneficiary Numbers | <input type="checkbox"/> Integrated Control Number (ICN) |
| <input type="checkbox"/> Partial Social Security Number | <input type="checkbox"/> Account Numbers | <input type="checkbox"/> Military History/Service Connection |
| <input type="checkbox"/> Date of Birth | <input type="checkbox"/> Certificate/License numbers ¹ | <input type="checkbox"/> Next of Kin |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Vehicle License Plate Number | <input type="checkbox"/> Date of Death |
| <input type="checkbox"/> Personal Mailing Address | <input type="checkbox"/> Internet Protocol (IP) Address Numbers | <input checked="" type="checkbox"/> Business Email Address |
| <input type="checkbox"/> Personal Phone Number(s) | <input type="checkbox"/> Medications | <input type="checkbox"/> Electronic Data Interchange Personal Identifier (EDIPI) |
| <input type="checkbox"/> Personal Fax Number | <input type="checkbox"/> Medical Records | <input type="checkbox"/> Other Data Elements (list below) |
| <input checked="" type="checkbox"/> Personal Email Address | <input type="checkbox"/> Race/Ethnicity | |
| <input type="checkbox"/> Emergency Contact Information (Name, Phone Number, etc. of a different individual) | <input type="checkbox"/> Tax Identification Number | |
| | <input type="checkbox"/> Medical Record Number | |

Other PII/PHI data elements: VA email address

1.2 What are the sources of the information in the system?

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

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?

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

Developers seeking VA Lighthouse API access or support with related issues submit basic contact information through an API signup form or Support Contact form on developer.va.gov. Information on these forms is collected directly from the developers to aid in ongoing API support. Once the information is relayed - via direct integration with LPB or through email-to-case workflows - a case is created within the Salesforce platform and tracked through various phases of support.

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.

Information from sources is not needed.

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

The system does not create information but aggregates various data points into reports and custom views.

1.3 How is the information collected?

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?

This tool does not collect information directly from end users (i.e., generally third-party developers). Information is received indirectly from upstream databases.

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 OMB Control number for the production signup, sandbox signup and support contact form is **2900-0700**.

1.4 How will the information be checked for accuracy? 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 accuracy of the information is dependent on the information provided by end users requesting access to APIs or contacting the API support team.

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?

No.

1.5 What specific legal authorities, arrangements, and agreements 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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 38, United States Code 501 (a).

Salesforce is the Cloud Service Provider however Salesforce does not maintain MOU/ISA, the interconnection resides within VA security boundaries. The VA owns the Authorized Boundary for the SFDP and the High environments with the "-E" ATO packages. The VA does not require an ISA/MOU for inter-connections between two or more VA-owned systems.

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. (Work with your System ISSO to complete this section)

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

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

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

*Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question 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:

Individual contact information is tracked in the Salesforce-VA lighthouse API support tool, and email

Version date: October 1, 2024

Page 7 of 28

correspondence on the type of support provided is tracked for each ticket/case submitted. The risk involves the PII information of the individuals being incorrectly provided when individuals submit the form.

Mitigation:

The VA support team reaches out to the user via user-reported email to respond to support requests. If the email address is invalid or the requesting individual fails to respond, the ticket is closed and the PII will no longer be used by VA. If they were not to receive an email about their support request, they can resubmit using the Developer portal support form.

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 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	Used as an identifier for the user submitting an access request or support inquiry	Not used
VA email address	Used as an identifier for the user submitting an access request or support inquiry	Not used
Personal email address	Used as an identifier for the user submitting an access request or support inquiry	Not used
Business email address	Used as an identifier for the user submitting an access request or support inquiry	Not used

2.2 What types of tools are 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?

Data ingested from upstream systems is not manipulated and enters Salesforce as raw data.

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 system does not create new information about individuals.

2.3 How is the information in the system 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?

The VA Lighthouse API Support team (Salesforce) is an encrypted secure system. Data in transit is protected by HTTPS site-to-site encryption. PII data is encrypted at rest with Salesforce Shield encryption.

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)

The system does not collect, process and/or retain SSNs.

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

OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006), reiterates and emphasizes agency responsibilities under law and policy to appropriately safeguard sensitive PII and train employees regarding their responsibilities for protecting privacy.

PII/PHI is safeguarded via HTTPS site-to-site encryption. PII data is encrypted at rest with Salesforce Shield encryption.

VA employees are required to complete mandatory, annual VA Privacy and Information Security Awareness and Rules of Behavior (WBT) and Privacy and HIPAA training courses.

VA Privacy and Information Security Awareness and Rules of Behavior (ROB) provides information security and privacy training important to everyone who uses VA information systems or VA sensitive information. The expectation is that after completing this course, VA employees will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements, and consequences and penalties for noncompliance; and explain how to report incidents.

VA Privacy and HIPAA training satisfies the mandatory requirement for all employees who have access to PHI and/or VHA computer systems during each fiscal year. This training provides guidance on privacy practices for the use and disclosure of protected health information (PHI) and Veteran rights regarding VHA data. It contains policy implementation content as described in VHA Handbook 1605.1.

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?

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for Information Technology [the VA Authorizing Official (AO)]. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans' information is used, stored, and protected.

Access Control:

Accessibility to data is granted based on the permission sets and role-based hierarchy applied based on FedRAMP Salesforce Gov Cloud Plus platform. Account creation is managed and offered through VA via two factor authentication (2FA). The managers will reject any applications from individuals who do not work with them, do not require access, or are not using the correct email address.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

How are they documented, i.e., Policy, SOP, other. And where is this documentation location?

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. VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems.

2.4c Does access require manager approval?

Yes, Lighthouse Public API Platform Product Owner approval is required for access.

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

Yes, there are logs for each access.

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

Information System Owner (ISO).

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*

Salesforce-VA Lighthouse API Support salesforce tool retains information of Veterans/ VA Employees/ Contractors/ Members of Public such as:

- First name
- Last name
- Personal, Business, or VA email address(es)

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. **The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.** 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.*

PII data retention period: Temporary; destroyed when business use ceases. (GRS 4.2 item 140, DAA-GRS-2013-0007-0013). Record Control Schedule 10-1 can be found at the following link: <https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf>

General Record Schedule: <https://www.archives.gov/records-mgmt/grs.html>

3.3 Has the retention schedule been 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 Privacy Officer and 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?

The information is retained following the policies and schedules of VA's Records management Service and NARA in "Department of Veterans Affairs Records Control Schedule 10-1".

3.3b Please indicate each record's retention schedule, series, and disposition authority?

GRS 4.2 item 140, DAA-GRS-2013-0007-0013; [Record Control Schedule 10-1](#).

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.

Salesforce-VA lighthouse API Support tool adheres to the VA RC Schedule 10-1. All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500. (https://www.va.gov/vapubs/search_action.cfm?dType=1).

The retention schedule for the Salesforce Government Cloud Plus (SFGCP) is also applied to VA Lighthouse API Support system. No paper form is used for tracking the case, the system undergoes an automatic purge of records as per SFGCP.

SFGCP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6500. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFDP records are retained according to Record Control Schedule 10-1 Section 4. (Disposition of Records)

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.

Salesforce-VA Lighthouse API Support does not use PII data stored in this application for research, testing or training.

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 ISSO 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: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described 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.

Privacy Risk: Depending on the retention time, PII information of the users submitting helpdesk requests are at risk of exposure to unauthorized individuals. The information is retained to assist users with existing issues with VA Lighthouse API.

Mitigation: All data at rest within the SFGCP security boundary is encrypted in accordance with FIPS 140-2, as well as protected by FedRAMP certified “HIGH” security controls. Use of FedRAMP HIGH controls implemented under the FedRAMP ATO. Collectively, these controls within the SFGCP security boundary provide maximum protection to all VA Salesforce data. Basic information and email correspondence about the submitted helpdesk ticket is retained.

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 (Servers/Database)

Salesforce - VA Lighthouse API Support consists of **one** 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 **Salesforce - VA Lighthouse API Support** 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
Salesforce VAPM Org	Yes	Yes	Name, Personal Email Address, Business Email Address, VA Email Address,	User Support Contact Information	System Owner Account Access Approval

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (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.

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
Digital Veterans Platform (DVP)	User Support Contact	Name, Personal Email, Business Email, VA Email Address	Salesforce calls LPB within the DVP boundary on an hourly basis to retrieve records

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure *Discuss the privacy risks associated with the sharing of information within the Department 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 inside the document in this section).*

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

Privacy Risk: The privacy risk associated with maintaining PII is that sharing data within the Department of Veterans’ Affairs could happen and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by the Lighthouse support staff. Only support staff with a clear business purpose is allowed access to the system and the information contained within.

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

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

Information is not shared outside of the Department, therefore there are no privacy risks.

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: Not applicable for the tool.

Mitigation: Not applicable for the tool.

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 Was notice provided to the individual before collection of the information? If yes, please provide a copy 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.

Yes, we provide a Privacy Act statement on all relevant forms. In addition, the associated SORN defines the information collected from Veterans/ VA Employees/ Contractors/ Members of Public, use of the information, and how the information is accessed and stored.

Please see screenshots in Appendix-A 6.1.

Case and Correspondence Management (CCM)–VA (75VA001B).
(<https://www.govinfo.gov/content/pkg/FR-2022-06-17/pdf/2022-13066.pdf>)

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.

Any form that requires the input of PII clearly states the Estimated burden, OMB Control number, Expiration date, and allows the end user to readily access the Privacy Act Statement.

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, the individuals can decline to provide the information requested by VA Lighthouse API Support on API signup and Developer portal support forms. If the individuals choose not to provide their information, then there is no assistance or support provided to them. The information requested on these forms is used to assist with access to and questions about VA-hosted APIs.

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 VA API Terms of Service page provides information on collection, usage, and privacy of individual data (<https://developer.va.gov/terms-of-service>). To request access to VA-hosted APIs or submit a support inquiry, users are required to review and agree to the aforementioned Terms of Service.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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 System ISSO to complete all Privacy Risk questions inside the document in this section).

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: 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: Risk pertains to individuals not knowing their PII information is being stored and tracked by the VA Lighthouse API Support application.

Mitigation: Two privacy notices are provided to users when they submit PII for support and API access requests: (1) on Terms of Service webpage (<https://developer.va.gov/terms-of-service>) which is required for submission and (2) and via privacy act statements that appear on form submission page. Additionally, notice through VA Privacy Service and this PIA provides a notice to the individuals that PII information such as name, contact information and work information is stored in Salesforce-VA Lighthouse API Support.

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 What are 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 \(efoia-host.com\)](https://efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.

There are no formal procedures in place for individual/developers to gain access to their information in

Salesforce-VA Lighthouse API Support. The information of developers/ individuals who submit their information through signup and support forms is collected to assist in obtaining access to and receiving requests about specific APIs; hence they do not require access to their information.

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)?

VA's Privacy Act regulations implementing the Privacy Act are 38 CFR §§ 1.575 – 1.582. VA regulations at [38 CFR § 1.582 – Exemptions](#) provide a complete listing of all VA exempt Privacy Act Systems of Records.

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

System 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.

The individuals can request to correct their information through email. VA employees and contractors that have access to the tool can correct the information within the Salesforce-VA Lighthouse API Support application.

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.

Individuals are informed on their completed or corrected information through email correspondence by the VA employees.

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 ensure data accuracy.***

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

An email request needs to be submitted to the OIT Product Engineering office for individuals to access their information. The administrator/ manager will then review each access request and process it accordingly. Alternatively, FOIA requests can be submitted for review and

information on the individual will be provided accordingly. FOIA requests and Web policies applicable for the tool can be accessed through <https://www.va.gov/webpolicylinks.asp>.

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 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: The risk pertains to individuals not knowing how to access, redress, and correct their information.

Mitigation: Individuals submitting a ticket to Salesforce-VA Lighthouse API Support, can access their information via email request. Subsequently, requests are validated by the manager of OIT Product Engineering. Approval to access or denial is communicated through email correspondence.

Per SORN, individuals seeking information on the existence and content of records in this system should contact the system manager in writing. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they 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?

Access is not permitted to non-government users. To obtain access, users submit access requests to system administrators. Additionally, users must obtain approval

from the supervisor/manager to gain access to the tool.

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?

Access is not permitted to users outside of VAPM and the Lighthouse program. Only assigned users can access this tool. Users must use Single Sign On (SSO) and two factor authentication to log into the Salesforce-VA Lighthouse API Support application.

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.

Types of Users and their role is listed below:

Role	Action
Support user	Read/ create/edit on each record, contacts, accounts, tasks status
Support Admin	Manage/ read/ create/ edit on each record.
Transfer case user	Permits users to transfer cases from queue/user to a different queue/user.

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

If so, 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.

Yes, VA contractors will have access to the tool. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the VA's Talent Management System (TMS).

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

Contractors have direct involvement with the design and maintenance of the system; however, all design and maintenance changes must be approved by the business owner of the system.

8.2c Does the contractor have a signed confidentiality agreement?

Yes.

8.2d Does the contractor have an implemented Business Associate Agreement for applicable PHI?

This is not applicable; PHI is not stored in the system.

8.2e Does the contractor have a signed non-Disclosure Agreement in place?

Yes.

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.

General Training includes VA Privacy and Information Security Awareness and Rules of Behavior (TMS 10176), VA On-Boarding enterprise-wide training, and information security training. Additionally, all new users accessing the VA Lighthouse API Support application undergo VA-Lighthouse program training.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

8.4a If Yes, provide:

1. The Security Plan Status: Approved
2. The System Security Plan Status Date: 06/22/2022
3. The Authorization Status: ATO
4. The Authorization Date: 6/13/2023
5. The Authorization Termination Date: 6/13/2026
6. The Risk Review Completion Date: 03/12/2021
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 No or In Process, provide your **Initial Operating Capability (IOC) date**.

N/A

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, the VA Lighthouse API Support system utilizes Salesforce Gov Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus.

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.

Yes, VA has full ownership of the PII that will be shared through the Salesforce-VA Lighthouse API support platform. Contract agreement “Salesforce Subscription Licenses, Maintenance and Support”, Contract Number: NNG15SD27B.

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.*

This is not applicable for the tool. VA has full ownership over the data stored in the Salesforce-VA Lighthouse API support system.

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.

VA has full authority over data stored in Salesforce-VA Lighthouse API Support application.

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).

Salesforce-VA Lighthouse API Support does not utilize RPA.

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
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 they provided in this Privacy Impact Assessment is true and accurate.

Privacy Officer, Gina Siefert

Information System Security Officer, James Boring

Information System Owner, Michael Domanski

APPENDIX A-6.1

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; screenshot of a website collection privacy notice).

Artifact A: <https://developer.va.gov/terms-of-service>


Artifact B:

Estimated burden: **9 minutes**

OMB Control #: **2900-0770**

Expiration date: **11/30/2026**

[View Privacy Act Statement](#)



Privacy Act Statement

This information is being collected in accordance with section 3507 of the Paperwork Reduction Act of 1995. VA may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB number. The estimated time needed to complete this form will average 9 minutes. Information gathered will be kept private and confidential to the extent provided by law. Completion of this form is voluntary.

Artifact C

Estimated burden: **6 minutes**

OMB Control #: **2900-0770**

Expiration date: **11/30/2026**

[View Privacy Act Statement](#)



Privacy Act Statement

This information is being collected in accordance with section 3507 of the Paperwork Reduction Act of 1995. VA may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB number. The estimated time needed to complete this form will average 6 minutes. Information gathered will be kept private and confidential to the extent provided by law. Completion of this form is voluntary.

HELPFUL LINKS:

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 Notice of Privacy Practices](#)

[VHA Handbook 1605.04: Notice of Privacy Practices](#)