



Privacy Impact Assessment for the VA IT System called:

**Lighthouse Public Platform**  
**Veterans Affairs Central Office (VACO)**  
**Product Engineering Services**  
**eMASS ID #2596**

Date PIA submitted for review:

2/6/2025

System Contacts:

*System Contacts*

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	<a href="mailto:gina.siefert@va.gov">gina.siefert@va.gov</a> oitprivacy@va.gov	224-558-1584
Information System Security Officer (ISSO)	Jeffrey Scott Gardiner	jeffrey.gardiner@va.gov	919-286-0411
Information System Owner	Andrew Fichter	andrew.fichter@va.gov	240-274-4459

## Abstract

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

The Lighthouse Public Platform (LHPP) enables VA developers to publish Application Programming Interfaces (APIs) that internal VA and third-party consumers can use to build software tools that serve Veterans, their families, and their advocates.

The Lighthouse Public Platform consists of a user-facing portal, web servers, backend application programming interfaces (APIs), databases, and document storage.

The VA API Developer Portal, [developer.va.gov](https://developer.va.gov), enables 3rd party developers to view API documentation, sign up for Sandbox access, and request Production Access.

## 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 Public Platform (LHPP) enables VA developers to publish Application Programming Interfaces (APIs) that internal VA and third-party consumers can use to build software tools that serve Veterans, their families, and their advocates.

- 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?*

Approximately 3000 sandbox developer sign-ups have occurred since 2018. These developers are both 3<sup>rd</sup> party and internal VA developers building applications leveraging VA APIs on the Lighthouse Public Platform.

Check if Applicable	Demographic of individuals
<input type="checkbox"/>	Veterans or Dependents
<input checked="" 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?*

Lighthouse Public Platform collects basic demographic information, e.g., name and email address, about developers to be able to provision Sandbox development credentials as well as to contact prospective consumers related to API's they are consuming.

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

Lighthouse Public Platform shares Sandbox sign-ups with its corresponding Salesforce integration (1951) in order to handle customer support requests as well as coordinate bulk API specific change notifications.

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

Yes.

c. *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?*

Lighthouse Public Platform is hosted in the Veterans Affairs Enterprise Cloud (VAEC) Amazon Web Services (AWS).

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

d. *What is the citation of the legal authority?*

- *5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By PublicLaw*

- No. 104---231, 110 Stat. 3048
  - 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
  - Public Law 100---503, Computer Matching and Privacy Act of 1988
  - E---Government Act of 2002 § 208
  - Federal Trade Commission Act § 5
  - 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
  - 146VA0005Q3 / 73 FR 16093 (03/26/2008); Department of Veteran's Affairs Identity Management System (VAIDMS) - VA
- I. What is the SORN?

This system does not retrieve information by a unique identifier therefore a SORN is not required.

J. 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 not in the process of being modified and a SORN does not exist.

#### 4. System Changes

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

Yes

No

if yes, <<ADD ANSWER HERE>>

e. 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:

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

Other PII/PHI data elements: <<Add Additional Information Collected but Not Listed Above Here (For Example, Biometrics)>>

**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.*

*1.2a 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 prospective developer provides their name, personal/business email address, and other non-PII information directly via self-service registration on developer.va.gov for Sandbox, as well as during the Production Access Request form for desired API(s).

*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*

<sup>1</sup> \*Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

*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 other than the individual is not required.

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

Yes. A sub-set of approved production consumers are listed on the VA.gov Apps You Can Use page provided to Veterans.

### **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 prospective developer provides this information directly via self-service registration on developer.va.gov.

*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?*

OMB Control #: **2900-0770**

### **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.*

The accuracy of the information is dependent on the information provided by the users requesting access to the APIs. It is not checked or validated against other source of information.

*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 system does not check for accuracy by using a commercial aggregator.

**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*

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).

**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 Public Platform processes Personally Identifiable Information (PII) which can be used to identify an individual, VA employee, or VA contractor. There is a risk that information contained within the systems could be inaccurate. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

**Mitigation:** The accuracy of the information is dependent on the information provided by the users requesting access to the APIs. Information entered by individuals is presumed to be

Version date: October 1, 2024

**Page 7 of 29**

accurate, complete, and current. Lighthouse Public Platform implements strict access control, security & rules of behavior training before access is available to members of the program and all access to PII is logged for traceability.

## 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	Identification of a Person	Not used
Personal Email Address	Contact information for prospective developer	Not used
Business Email Address	Contact information for prospective developer	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?*

Lighthouse Public Platform does not conduct any analysis.

*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.*

Lighthouse Public Platform does not create any new information about an individual.

### 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 in transit is encrypted in transit with TLS 1.2+ and uses authenticated access (i.e API Keys and OAuth 2.0 Access Tokens). Data at rest is stored with industry standard AES-256 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).*

Lighthouse Public Platform does not utilize SSN.

*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.

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?*

Lighthouse Public Platform grants access using the principle of least privilege; only granting access to the data requested by the consumer and approved by the System Owner. Admin users are explicitly enabled and require VA network to access PII data. System integrations are granted an API key for explicit endpoint(s) that minimize data shared.

*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 privacy controls are implemented 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. New integrations require System Owner approval. Admin access requires full VA team onboarding an explicit access control list (ACL) addition to then log in with single sign on (SSO) with two factor auth enabled.

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

Yes. There are logs for each API call as well as Admin console logs.

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

The 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*

Name, Personal Email Address, Business Email Address

### **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.*

This information is retained indefinitely. Consumers have the ability to reach out to Lighthouse Public Platform to request deletion and procedures are in place.

### **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?*

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 records 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.*

The system identifies and deletes developer accounts that have over 6 years of inactivity.

Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle Bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

[https://www.va.gov/vapubs/search\\_action.cfm?dType=1](https://www.va.gov/vapubs/search_action.cfm?dType=1).

### **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.*

Lighthouse Public Platform does not use PII 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 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:** There is a risk that the information maintained by the system could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at

greater risk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

**Mitigation:** Lighthouse Public Platform minimizes this risk by collecting the minimum required information prospective consumers at the self-service Sandbox step. Additionally, the data in transit is protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in transit protection standards. All Sandbox data accessible is also mocked.

## 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 **Lighthouse Public Platform** consists of 1 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 **Lighthouse Public Platform** 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*

<b>Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI</b>	<b>Does this system collect PII? (Yes/No)</b>	<b>Does this system store PII? (Yes/No)</b>	<b>Type of PII (SSN, DOB, etc.)</b>	<b>Reason for Collection/Storage of PII</b>	<b>Safeguards</b>
Lighthouse Platform Backend	Yes	Yes	Name Personal Email Address Business Email Address VA Email Address	Contact information for prospective API consumer	HTTPS, encryption at rest

**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*

<i><b>IT system and/or Program office. Information is shared/received with</b></i>	<i><b>List the purpose of the information being shared /received with the specified program office or IT system</b></i>	<i><b>List PII/PHI data elements shared/received/transmitted.</b></i>	<i><b>Describe the method of transmittal</b></i>
Salesforce (1951) - VA Lighthouse API Support	Shared to enable customer support team to communicate with target consumer groups by API registration.	Name Personal Email Address Business Email Address VA Email Address	HTTPS, API key restricted

**4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

*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:** Lighthouse Public Platform processes PII through sharing of information with other VA systems. This presents the risk that information may be disclosed to individuals who have no requirement for this information which heightens the threat of information being misused.

**Mitigation:** Lighthouse Public Platform adheres strictly to the principle of need-to-know. All staff is required to complete the VA Privacy training and granted access only to information with a clear business purpose. Additionally, sharing across the system boundary requires an isolated API key.

## 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</i>	<i>List the purpose of information</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted)</i>	<i>List agreements such as:</i>	<i>List the method of transmission</i>
--	--	---	---------------------------------	--



<i>information is shared/received with</i>	<i>being shared / received / transmitted</i>		<i>Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)</i>	<i>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.*

*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:** Lighthouse Public Platform does not provide direct external sharing of information.

**Mitigation:** Lighthouse Public Platform does not provide direct external sharing of information.

**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.*

#### 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.

*6.1b If notice was not provided, explain why.*

Notice was provided.

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

Lighthouse Public Platform includes a Terms of Service and specific Privacy Act Statement notice before collecting Sandbox registration and Production access request information.

#### **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. If the prospective consumer can elect to not share their information as part of Sandbox registration / Production Access request. Yes, Terms of Service acknowledgement is required before submission is accepted.

#### **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.*

No. The Terms of Service do not offer filtered options for consent. It is either full approval or the system cannot be accessed.

#### **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 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:*

*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:** There is a risk that VA Employees, Contractors, and Individuals will not know how their information is stored and used within VA.

**Mitigation:** Lighthouse Public Platform mitigates this risk by including an explicit & required terms of service consent as well as a Privacy Act Statement as part of both Sandbox sign-up and Production Access Request flows that collect PII. Additionally, the Public Posting of this PIA explains how information is stored and used within the VA.

### **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 \(efoia-host.com\)](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 Lighthouse Public Platform. 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 covers 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 Lighthouse Public Platform is fully self-service allowing the consumer to follow-up with a corrected Sandbox sign-up or Production Access Request. Additionally, they can reach out via the Developer Portal contact page (<https://developer.va.gov/support/contact-us>) to request updates/corrections if desired.

## **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 Public Platform terms of service, <https://developer.va.gov/terms-of-service>, specify that “Any registration information you give to VA must be accurate and up to date and you must inform us promptly of any updates so that we can keep you informed of any changes to the API or the Terms which may impact your usage of the API.”. This can be done via the Contact page on the Developer Portal, or via the contact email provided during sign-up.

## **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.*

Individuals can reach out via the Developer Portal contact page (<https://developer.va.gov/support/contact-us>) or via the support email address provided during sign-up.

### **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 VA Employees, Contractors, or Individuals whose records contain incorrect information may not receive notification of any changes.

**Mitigation:** Lighthouse Public Platform offers self-service Sandbox allows for new sign-ups with corrected information as well as a customer support team that responds to Contact Us form and support mailbox in a timely manner to support any requested updates/corrections.

## **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 Lighthouse Public Platform team member. Accounts ultimately need to be approved by the System Owner before they are created. Once created, an existing Lighthouse Public Platform administrator can grant access via (Single Sign-On) SSO with (multifactor authentication) MFA to the Admin Console only if there is a need-to-know.

*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?*

No users from other agencies have access to the Lighthouse Public Platform system.

*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.*

Lighthouse Public Platform restricts access to Administrators for Admin Console read/write. Additionally, API keys can be created for specific system interactions.

## **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.*

Yes. VA contractors have annually enforced trainings including Rules of Behavior & VA Privacy and Security Training. Privacy and security training are enforced annually and must be completed for the contractors' continued access to be approved by the System Owner. All contractors must have a public trust clearance to access the system as well.

*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?*

No, there is no Business Associate Agreement as it is not required as there is no access to PHI. All contractors must have a public trust clearance in place to access the system and PII, and the ISO must approve their access. The following privacy training courses are required to be taken annually, and completion certifications are recorded:

- VA Privacy and Information Security Awareness and Rules of Behavior

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?

VA Contractors work directly with the System Owner to design, implement, and provide ongoing support & 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.*

For Lighthouse Public Platform staff, all employees adhere to the VA mandated trainings before accounts are provisioned to access Lighthouse Public Platform resources: Rules of Behavior, Two Factor Authentication, VA Privacy and Security Training, VA Safeguard and Awareness Training. Privacy and security trainings are enforced annually and must be completed for contractors' continued access to be approved by the System Owner.

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

8.4a If completed, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<ADD ANSWER HERE>>

*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.**

In Process of migration to isolated ATO. Categorized as a **Moderate** system with an IOC – March 31, 2025.

## **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)*

Lighthouse Public Platform is a *Platform as a Service (PaaS)* running in the VA-authorized and controlled Cloud Computing Environment, Veterans Affairs Enterprise Cloud (VAEC) Amazon Web Services (AWS). The system and data will reside in the VAEC AWS GovCloud environment. VA Enterprise Cloud’s AWS platform and associated services leveraged are categorized FedRAMP High.

**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. Amazon Web Services (AWS) GovCloud. VA-118-16-D-1015.

**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.*

No ancillary data is collected.

**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.*

Lighthouse Public Platform data held by the cloud provider is the contractor's responsibility to design, maintain, and protect. The cloud provider may hold logs of calls made the underlying system components.

**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).*

Lighthouse Public Platform does not use any Robotics Process Automation.



## Section 10. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

<b>ID</b>	<b>Privacy Controls</b>
<b>AP</b>	<b>Authority and Purpose</b>
AP-1	Authority to Collect
AP-2	Purpose Specification
<b>AR</b>	<b>Accountability, Audit, and Risk Management</b>
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
<b>DI</b>	<b>Data Quality and Integrity</b>
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
<b>DM</b>	<b>Data Minimization and Retention</b>
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
<b>IP</b>	<b>Individual Participation and Redress</b>
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
<b>SE</b>	<b>Security</b>
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
<b>TR</b>	<b>Transparency</b>
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
<b>UL</b>	<b>Use Limitation</b>
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.**

---

**Privacy Officer, Gina Siefert**

---

**Information Systems Security Officer, Jeffrey Scott Gardiner**

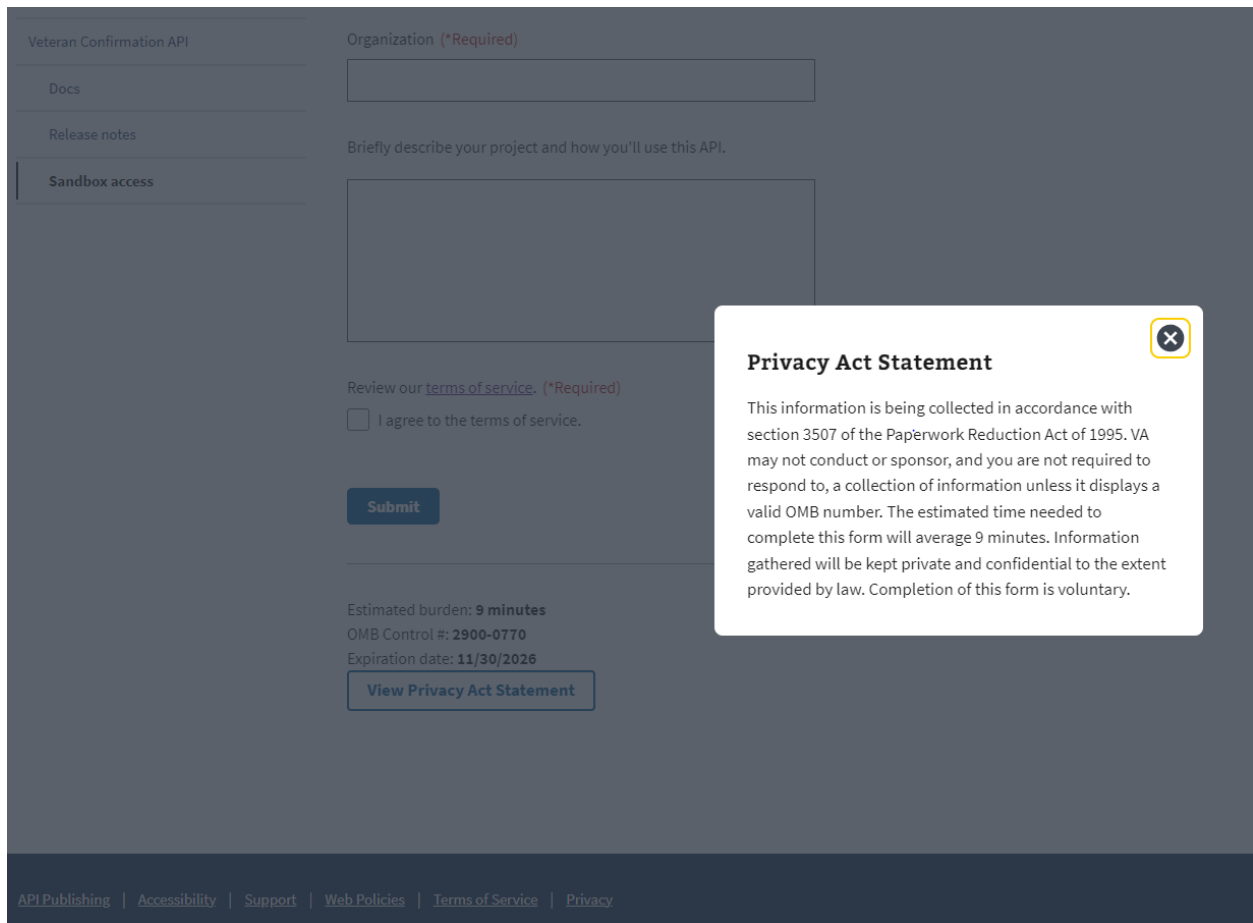
---

**Information Systems Owner, Andrew Fichter**

## APPENDIX A-6.1

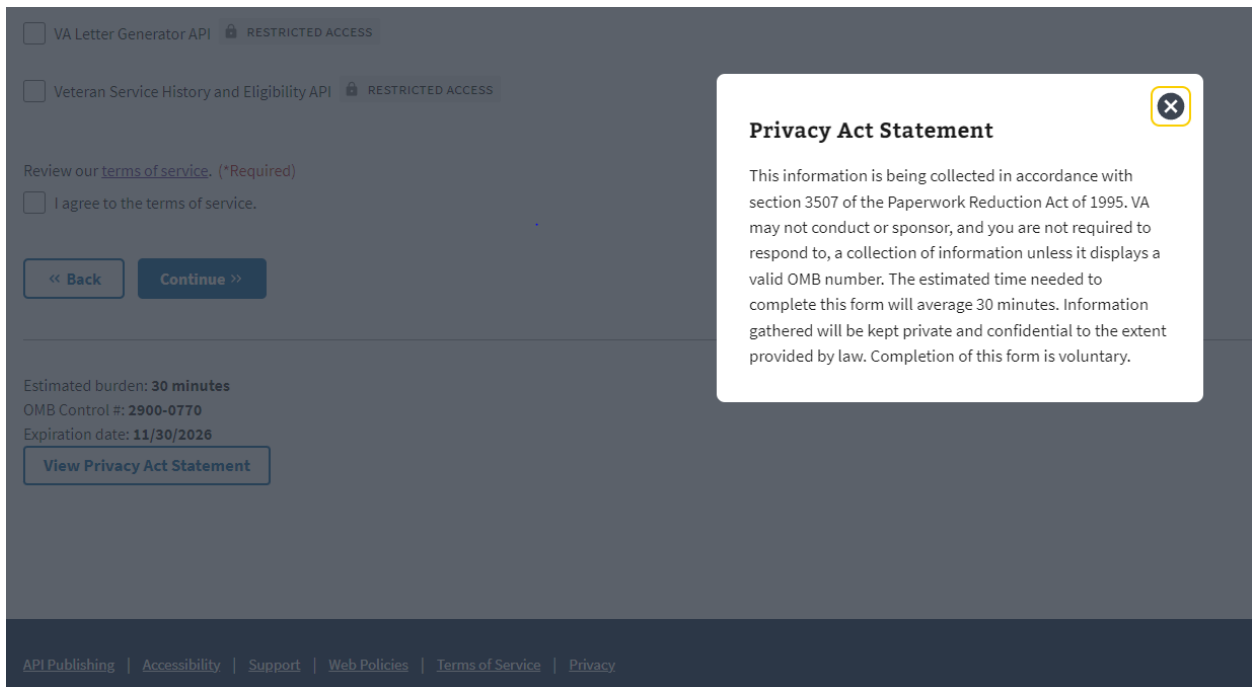
Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

Below shown as part of the Developer Portal Sandbox sign-up form.



The image shows a screenshot of a web form for the "Veteran Confirmation API" sandbox. The form includes a sidebar with links for "Docs", "Release notes", and "Sandbox access". The main content area has a "Organization (\*Required)" field, a "Briefly describe your project and how you'll use this API." text area, and a "Review our [terms of service](#). (\*Required)" section with an "I agree to the terms of service." checkbox. A "Submit" button is located below the checkbox. At the bottom of the form, it states "Estimated burden: 9 minutes", "OMB Control #: 2900-0770", and "Expiration date: 11/30/2026", with a "View Privacy Act Statement" button. A white "Privacy Act Statement" overlay is positioned on the right side of the form, containing the following text: "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." The overlay has a close button in the top right corner. At the bottom of the page, there is a footer with links for "API Publishing", "Accessibility", "Support", "Web Policies", "Terms of Service", and "Privacy".

Below is from the Production Access request page.



Terms of Service link in the above screenshots.

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

## **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 \(va.gov\)](#)