Privacy Impact Assessment for the VA IT System called:

Lighthouse Fast Healthcare Interoperability Resources API

Veterans Affairs Central Office (VACO)

Product Engineering Services

eMASS ID # 2392

Date PIA submitted for review:

12/27/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	Gina.siefert@va.gov 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 Fast Healthcare Interoperability Resources API is a set of cloud-enabled Software as a Service (Saas) services. These APIs provide an industry standards-based view of VA Healthcare data. This is accomplished by aggregating VA Healthcare data, transforming the data to the industry standard Health Level Seven (HL7) FHIR format, and returning the data to VA Applications and/or approved third-party consumer applications. Providing APIs for this data enables consumers to build applications using VA Healthcare data for the benefit of both Veterans and the VA.

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?*

Lighthouse Fast Healthcare Interoperability Resources API (LHFHIR) provides industry standard interfaces to VA healthcare data which enables consumers (internal VA and commercial third parties) to build applications using VA Healthcare data for the benefit of both Veterans and the VA.

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?

Lighthouse Fast Healthcare Interoperability Resources API does not store data on individuals. Lighthouse Fast Healthcare Interoperability Resources API provides programming interfaces allowing approved applications to access VA Patient Healthcare related data. The system allows for other approved applications to provide rich experiences for the VA Patients and clinicians through secure access to VA Electronic Health Record (EHR) data.

Check if Applicable

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

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

Lighthouse Fast Healthcare Interoperability Resources API provides access to the VA medical records including data such as: Allergies, Health Conditions and Diagnoses, Medical test results, vaccinations, medication details, prescriptions, self-reported medications, surgeries, medical devices, appointments, medical visits, clinical notes, and financial information like medical insurance debts and payments using Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) standards for interoperability. The system provides interoperable access to this data to enable VA and third-party applications to provide value-added experiences with this information for VA patients and clinicians.

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

The Lighthouse Fast Healthcare Interoperability Resources API provides read-only access to VA EHR data including data such as: Allergies, Health Conditions and Diagnoses, Medical test results, vaccinations, medication details, prescriptions, self-reported medications, surgeries, medical devices, appointments, medical visits, clinical notes, and medical insurance related financial information like debts and payments using Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) standards for interoperability. This data is sourced from VA sources such as Corporate Data Warehouse (CDW), Veterans Health Information Systems and Technology Architecture (VistA), Health Data Repository (HDR), Master Person Index (MPI), and DoD source Oracle Health, and is shared with authorized third-party commercial applications based on direct consent of individuals or established data sharing agreements with the VA in compliance with the ONC 21st Century Cures Act, as well as, other authorized internal VA application which need access to the medical record data to serve their users such as clinicians.

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

The purpose of the data sources the LHFHIR API connects to is to share the EHR information the API serves. The API's connection to these sources is constant, to enable the supply of data our API serves, making these modules always applicable to the system.

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

Lighthouse Fast Healthcare Interoperability Resources API is hosted in the Veterans Affairs Enterprise Cloud (VAEC) Amazon Web Services (AWS). The system is operated in the AWS us-gov-west-1 Region, and uses three Availability Zones: usgw1-az1, usgw1-az2, and usgw1-az3. The system is not operated in more than one site, meaning it does not operate outside of the AWS Cloud.

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

H. What is the citation of the legal authority?

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law
- 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
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws
- The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 9397

I. What is the SORN?

- 121VA10 / 88 FR 22112 (4/12/2023); National Patient Databases – VA AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
    - 38 U.S.C 501
- 24VA10A7 / 85 FR 62406 (10/2/2020); Patient Medical Records – VA AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
    - Title 38, United States Code, Sections 501(b) and 304
- 79VA10 / 85 FR 84114 (12/23/2020); Veteran Health Information Systems and Technology Architecture (VistA) Records – VA
- 146VA0005Q3 / 73 FR 16093 (03/26/2008); Department of Veteran's Affairs Identity Management System (VAIDMS) - VA

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

SORNs applicable to Lighthouse Fast Healthcare Interoperability Resources API (LHFHIR) do not require amendment or revision or approval. All applicable SORNs cover cloud usage and storage.

4. System Changes

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

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

L. *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://vawww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.*

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

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

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

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

Other PII/PHI data elements:

- National Provider Identifier (NPI)
- Business Phone Numbers
- Business Fax Numbers

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?

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

Lighthouse Fast Healthcare Interoperability Resources API does not store data, nor does it collect data from individuals. The system provides application programming interfaces to VA sources of this data such as CDW, VistA, HDR, and MPI, and DoD source Oracle Health. The Lighthouse Fast Healthcare Interoperability Resources API access data from these systems and present the information to the authorized consumers of the API using HL7 FHIR data standards.

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.

Lighthouse Fast Healthcare Interoperability Resources API serves data to allow for consistent reliable sharing of medical information so Patients can access their medical record (through other applications) in accordance with the ONC 21st Century Cures Act and to standardize access to the medical record for applications being developed for use within the VA EHR.

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

Lighthouse Fast Healthcare Interoperability Resources API does not create information.

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?

Lighthouse Fast Healthcare Interoperability Resources API accesses information from other VA systems such as CDW through secure SQL database connection, VistA instances through VistALink, direct TCP connections, HDR through SOAP APIs, and MPI through SOAP APIs. The API also accesses information from DoD system Oracle Health through OAuth 2.0 Client Credentials Grant over HTTPS. Information processed is safeguarded in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data processing standards.

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

Lighthouse Fast Healthcare Interoperability Resources API does not collect information on any forms.

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.

Lighthouse Fast Healthcare Interoperability Resources API is not storing information directly. The integrity of the data is based on the integrity controls in place at the data sources used by the system. All information is checked at the source end. Information processed is safeguarded in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data processing standards.

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?

Lighthouse Fast Healthcare Interoperability Resources API does not have checks for accuracy of the data in the source systems from which it accesses information.

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

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law
- 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
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws
- The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 9397
- 121VA10 / 88 FR 22112 (4/12/2023); National Patient Databases – VA AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
    - 38 U.S.C 501
- 24VA10A7 / 85 FR 62406 (10/2/2020); Patient Medical Records – VA AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
    - Title 38, United States Code, Sections 501(b) and 304
- 79VA10 / 85 FR 84114 (12/23/2020); Veteran Health Information Systems and Technology Architecture (VistA) Records – VA
- 146VA0005Q3 / 73 FR 16093 (03/26/2008); Department of Veteran's Affairs Identity Management System (VAIDMS) - VA

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: 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: Lighthouse Fast Healthcare Interoperability Resources API processes Personally Identifiable Information (PII) and Personal Health Information (PHI) which can be used to identify a Veteran, VA Patient or individual.

LHFHIR API processes and transmits healthcare records including Diagnoses, Prescriptions, medications, clinical notes, etc. Unauthorized modification or destruction of health care information may result in incorrect, inappropriate, or excessively delayed treatment of patients. The system exchanges VA information between VA systems and the accuracy of the data is dependent on the source system.

Mitigation: Data Processed by Lighthouse Fast Healthcare Interoperability Resources API is protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards.

Data LHFHIR API receives from backend data sources is in read-only format, and healthcare professionals double-check its accuracy before making any decisions. In the event the data is altered, the correct data can be retrieved from the authoritative EHR sources like VistA, which minimizes adverse impacts on VA operations, assets, or individuals.

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 Demographic Information returned about a Patient	Demographic Information returned about a Patient
Social Security Number	Demographic Information returned about a Patient	Demographic information returned about a Patient
Date of Birth	Identification of a Person Demographic Information returned about a Patient	Demographic information returned about a Patient
Mother's Maiden Name	Identification of a Person Demographic Information returned about a Patient	Demographic information returned about a Patient
Personal Mailing Address	Identification of a Person Demographic Information returned about a Patient	Demographic information returned about a Patient
Personal Phone Number (s)	Demographic Information returned about a Patient	Demographic information returned about a Patient
Personal Fax Number	Demographic Information returned about a Patient	Demographic information returned about a Patient
Personal Email Address	Demographic Information returned about a Patient	Demographic information returned about a Patient
Emergency Contact Information	Demographic Information returned about a Patient	Demographic Information returned about a Patient
Medications	Demographic Information returned about a Patient	Medical data returned about a Patient
Medical Records	Medical data returned for an authorized clinician to view	Medical data returned for the Patient and/or authorized clinician to view
Race/Ethnicity	Demographic Information returned about a Patient	Demographic Information returned about a Patient
Gender	Identification of a Person Demographic Information returned about a Patient	Demographic Information returned about a Patient
Integrated Control Number (ICN)	Identification of a Person	Identification of a Person
Medical Record Number	Used to identify a Patient	Used to identify a Patient

Next of Kin	Demographic Information returned about a Patient	Demographic Information returned about a Patient
Electronic Data Interchange Personal Identifier (EDIPI)	Identification of a Person	Not Used
Business Phone Number (s)	Not Used	Used to share how to contact a VA Organization or Practitioner
Business Fax Number (s)	Not Used	Used to share how to contact a VA Organization or Practitioner
Business Email Address	Not Used	Used to share how to contact a VA Organization or Practitioner
National Provider Identifier (NPI)	Identification of a VA Practitioner	Identification of a VA Practitioner
Financial Information	Financial information returned about a Patient's medical debts and medical payments	Financial information returned for the Patient to view about their medical debts and medical payments
Health Insurance Beneficiary Account Numbers	Identifier of a VA Patient's health insurance account	Used to identify a VA Patient's health insurance account so the Patient may manage their healthcare expenses

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 Fast Healthcare Interoperability Resources API is middleware and does not create information. The system exchanges information between internal VA systems and approved (by VA Product Engineering Services) third-party commercial and internal VA API consumers. Lighthouse Fast Healthcare Interoperability Resources API may contain PII and PHI. The only transformations of data performed are to align the VA data with Health Level Seven (HL7) International Fast Healthcare Interoperability Resources (FHIR) standards. These transformations are established based on collaboration with the VA Knowledge Based Systems (KBS) terminology team. The services provided by Lighthouse Fast Healthcare Interoperability Resources API do not provide or replace the consultation, guidance, or care of a health professional or other qualified provider. Healthcare providers should consult with authoritative records when making decisions.

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 Fast Healthcare Interoperability Resources API does not create any new information.

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). There is no data at rest within the system.

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

No additional SSN protections are in place beyond being encrypted in transit using FIPS 140-2 compliant algorithms and only being available to certain users.

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

Lighthouse Fast Healthcare Interoperability Resources API runs within the VAEC AWS cloud and therefore satisfies the requirements of OMB Memorandum M-06-15

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

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

<u>Principle of Use Limitation:</u> 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 Fast Healthcare Interoperability Resources API grants access using the principle of least privilege; only granting access to the data requested by the consumer, consented by the individual and approved by the System Owner. For third-party commercial consumers, the individual requesting access to their data via the application that integrates with the system must be provided the ability to revoke their consent at any time. Alternatively, the third-party commercial consumer may establish an explicit sharing agreement with the VA (e.g. ISA/MOU, CRADA). API credentials are only issued after the System Owner approves access.

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 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, System 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 of the API.

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

None

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.*

Data passes through Lighthouse Fast Healthcare Interoperability Resources API transiently upon individual requests and is not retained within the system.

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?

Lighthouse Fast Healthcare Interoperability Resources API does not store information.

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

Lighthouse Fast Healthcare Interoperability Resources API does not store information.

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.

Lighthouse Fast Healthcare Interoperability Resources API does not store information.

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 Fast Healthcare Interoperability Resources API provides a Sandbox testing environment for consumers without PII and PHI. The Sandbox environment models Production functionality and data using synthetic test data. The data in Sandbox mimics Production data but contains no real patient data. This makes Sandbox safe for research, testing, or training with zero risk of compromising PII.

<u>3.6 PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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 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: Lighthouse Fast Healthcare Interoperability Resources API does not store information.

Mitigation: Lighthouse Fast Healthcare Interoperability Resources API mitigates risk of stored information by only handling data transiently per request following the principle of minimization by identifying that the data need not be held within the system. Additionally, the data in transit through the system is protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in transit protection standards.

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 Fast Healthcare Interoperability Resources API consists of 4 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 Fast Healthcare Interoperability Resources API 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**
Clinical Health API	**Yes**	**No**	• Name • Social Security Number (SSN) • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Medications • Medical Records • Race/Ethnicity • Gender	The Clinical Health API provides this information from the VA Electronic Health Records to ensure the information can be shared securely when needed in clinical contexts**.**	Data in transit is protected using encryption in accordance with FIPS 140-2

			• Integrated Control Number (ICN) • Next of Kin • Business Phone Number (s) • Business Fax Number (s) • Business Email Address • National Provider Identifier (NPI) Medical Record Number		
Patient Health API	**Yes**	**No**	• Name • Social Security Number (SSN) • Date of Birth • Mother’s Maiden Name • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Medications • Medical Records	The Patient Health API provides this information from the VA Medical record to empower individuals with access to their own data safely and securely.	Data in transit is protected using encryption in accordance with FIPS 140-2

			• Race/Ethnicity • Gender • Integrated Control Number (ICN) • Next of Kin • Electronic Data Interchange Personal Identifier (EDIPI) • Business Phone Number • Business Fax Number • Business Email Address • National Provider Identifier (NPI) • Medical Record Number		
Provider Directory API	**Yes**	**No**	• Name • Gender • Integrated Control Number (ICN) • Business Phone Number (s) • Business Fax Number (s) • Business Email Address • National Provider Identifier (NPI)	The Provider directory provides access to this data on VA providers in support of publishing available healthcare within the VA.	Data in transit is protected using encryption in accordance with FIPS 140-2

			• Medical Record Number		
Health Care Costs and Coverage API	**Yes**	**No**	• Name • Race/Ethnicity • Gender • Integrated Control Number (ICN) • Social Security Number (SSN) • Date of Birth • Mother’s Maiden Name • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Medications • Medical Records • Medical Record Number • Financial information • Health Insurance Beneficiary	The Health Care Costs and Coverage API provides information about VA Patients’ healthcare insurance expenses such as out-of-pocket costs and payment accuracy, making it more understandable and manageable for the Patient.	Data in transit is protected using encryption in accordance with FIPS 140-2

			Account Numbers		

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

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

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Veteran Health Administration (VHA) Corporate Data Warehouse (CDW)	Source of the information being made available via the APIs.	• Name • Social Security Number (SSN) • Date of Birth • Mother's Maiden Name • Personal Mailing Address	SQL Server Connection (Windows authentication/Kerberos)

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		• Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information ((Name, Phone Number, etc. of a different individual) • Medications • Medical Records • Race/Ethnicity • Gender • Integrated Control Number (ICN) • Next of Kin • Business Phone Number(s) • Business Fax Number (s) • Business Email Address • National Provider Identifier (NPI) • Medical Record Number	
Office of Information and Technology (OI&T) Master Person Index (MPI)	Uniquely identify users and access correlated identifiers for the person.	• Name • Social Security Number (SSN) • Date of Birth • Mother's Maiden Name	HTTPS

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		• Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Race/Ethnicity • Gender • Integrated Control Number (ICN) • Electronic Data Interchange Personal Identifier (EDIPI) • National Provider Identifier (NPI)	
Veteran Health Administration (VHA) Health Data Repository (HDR)	Access Clinical Notes to be served by the APIs.	• Medical Records • Integrated Control Number (ICN)	HTTPS
Veteran Health Administration (VHA) Veteran Health Information Systems and Technology Architecture (VistA)	Source of the information being made available via the APIs.	• Medications • Medical Records • Integrated Control Number (ICN)	TCP
Office of Information and Technology (OI&T)	DVP controls the API Gateway through which incoming traffic	• Name • Social Security Number (SSN)	HTTPS

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Digital Veterans Platform (DVP)	passes to reach the Lighthouse Fast Healthcare	• Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Medications • Medical Records • Race/Ethnicity • Gender • Integrated Control Number (ICN) • Next of Kin • Electronic Data Interchange Personal Identifier (EDIPI) • Business Phone Number(s) • Business Fax Number(s) • Business Email Address • National Provider Identifier (NPI) • Medical Record Number	

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***

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

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

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

Follow the format below:

<u>Privacy Risk:</u> Lighthouse Fast Healthcare Interoperability Resources API process both PII and PHI through sharing of information with other VA systems. This presents the risk that the information may be disclosed to individuals who have no requirement for this information which heightens the threat of information being misused.

<u>Mitigation:</u> Lighthouse Fast Healthcare Interoperability Resources API adheres strictly to the principle of need-to-know. All staff is required to complete VA Privacy and HIPAA training and are granted access only to information with a clear business purpose.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

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

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Oracle Health (DoD owned/operated)	To allow Va Patients to access their EHR data from VA Medical Centers that have been modernized to Oracle Health	• Name • Social Security Number (SSN) • Date of Birth • Mother’s Maiden Name • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Medications • Medical Records • Race/Ethnicity	Authority To Connect	OAuth 2.0 Client Credentials Grant over HTTPS

		• Gender • Integrated Control Number (ICN) • Next of Kin • Business Phone Number (s) • Business Fax Number (s) • Business Email Address • National Provider Identifier (NPI) • Medical Record Number		

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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:

<u>Privacy Risk:</u> Lighthouse Fast Healthcare Interoperability Resources API does not provide direct external sharing of information.
Oracle Health is a backend data source from which LHFHIR API receives information. The sharing of information is unidirectional coming into VA from Oracle Health. The LHFHIR API does not share information with Oracle Health. This external connection to Oracle Health results in DoD providing LHFHIR API with VA data due to the shared Electronic Health Record which is read only.
If the VA and DoD systems are not aligned on common patient identifiers, there is a possible risk that mismatches could occur, resulting in one patient's medical records being exposed to a different patient as their own.

<u>Mitigation:</u> Lighthouse Fast Healthcare Interoperability Resources API does not provide direct external sharing of information.
To mitigate the risk in the event the VA and DoD systems are not aligned on common patient identifiers, Lighthouse Fast Healthcare Interoperability Resources API correlates identity

between the systems using Master Person Index (MPI) to ensure the patient record being returned does indeed belong to the patient for whom the request is being made.

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.

Lighthouse Fast Healthcare Interoperability Resources API does not collect PII information. It sources VA Patient medical record information from systems within the VA such as CDW, VistA, HDR, MPI, and DoD Oracle Health and passes this information through to authorized consumers. Lighthouse Fast Healthcare Interoperability Resources API defers collection notification to its data source systems. Privacy Notice is served by the data source system at time of collection and/or through the data source systems' PIAs and SORNs. For third-party applications that use Lighthouse Fast Healthcare Interoperability Resources API the users are prompted to provide revokable consent for information requested by the consumer application in addition to the third-party application's Terms of Service and Privacy Policy. For applications that attended by the users a documented agreement such as an ISA/MOU or CRADA is established. This Privacy Impact Analysis (PIA) also serves as notice of the Lighthouse Fast Healthcare Interoperability Resources API Assessing as required by the eGovernment Act of 2002, Pub.L.107-347 208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of agencies. VA System of Record Notices (SORNs) which are published in the Federal Register and available online.

6.1b If notice was not provided, explain why.

Lighthouse Fast Healthcare Interoperability Resources API does not collect PII information. LHFHIR API defers collection notification to its data source systems The notice is provided by the data source system at the time of collection and/or through those systems' PIAs and SORNs.

Notice is provided as part of the Privacy policy of the consumers of the API and users are prompted to provide revokable consent. This Privacy Impact Analysis (PIA) also serves as notice of the Lighthouse Fast Healthcare Interoperability Resources API Assessing as required by the eGovernment Act of 2002.

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

Lighthouse Fast Healthcare Interoperability Resources API does not collect PII information. LHFHIR API defers collection notification to its data source systems. Privacy Notice is served by the data source system at time of collection and/or through the data source systems' PIAs and SORNs.

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.

VHA Directive 1605.1 section 5 “Individual’s Rights” lists the rights of the Veterans to request VHA restrict the uses and/or disclosures of the individual’s individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR Version Date: October 1, 2015 1.575(a)). Individuals do have an opportunity to decline to provide information at any time. There is no penalty or denial of service for declining to provide information. The Privacy Right to decline to provide information is handled by the specific source system that collects the information.

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.

Individuals have the right to consent to particular uses of information. Individuals are directed to use the Request for Authorization to Release Medical Records Form (VA Form 10-5345) describing what information is to be sent out and to whom it is being sent. Patients have the right to opt-out of VA facilities directories. VHA Directive 1605.1 section 5 “Individual’s Rights” lists the rights of the Veterans to request VHA restrict the uses and/or disclosures of the individual’s individually identifiable health information to carry out treatment, payment, or health care operations.

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 and Individuals will not know that applications built using Lighthouse Fast Healthcare Interoperability Resources API process or contain PII, PHI, and other Sensitive Personal Information (SPI) about them.

Mitigation: Lighthouse Fast Healthcare Interoperability Resources API mitigates this risk by ensuring that individuals are provided notice of information and notice of the system's existence. Also to mitigate this risk the PIA is made available to the public, and the applicable source systems' SORNs are published in the federal registrar.

Section 7. Access, Redress, and Correction

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

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

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

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

Lighthouse Fast Healthcare Interoperability Resources API does not store or retain information. The system provides application programming interfaces to VA sources of this data such as CDW, VistA, HDR, and MPI, and DoD source Oracle Health. The Lighthouse Fast Healthcare Interoperability Resources API access data from these systems and present the information to the authorized consumers of the API using HL7 FHIR data standards.
The accuracy of the data is dependent on the source system. LHFHIR API does not have write capabilities to edit patient records. In the event a patient's record is determined to be inaccurate, it must be corrected by the authoritative source system. Veterans may amend their records via submitted written request. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement.

Similarly, when requesting access to one's own records, patients are asked to complete VA Form 10-5345a: Individuals' Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at https://www.va.gov/health-care/get-medical-records/. Additionally, Veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the My HealtheVet program, VA's online personal health record. For more information about My HealtheVet at https://www.myhealth.va.gov/index.html. VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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)?

Lighthouse Fast Healthcare Interoperability Resources API is not exempt from the Privacy Act.

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

Lighthouse Fast Healthcare Interoperability Resources API 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.

Lighthouse Fast Healthcare Interoperability Resources API consists of APIs and information is passed transiently through the system. The following procedures reference what is necessary to correct information in the source data systems in use such as Corporate Data Warehouse, VistA, Health Data Repository, and Master Patient Index. In accordance with VHA Directive 1605.1 section 8.a "Right to Request Amendment of Records" states the rights of the Veterans to amend to their records via submitted written request. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

Lighthouse Fast Healthcare Interoperability API is a set of APIs and does not control the data directly. Correction of data is controlled through the various source systems such as the Corporate Data Warehouse, VistA, Health Data Repository and Master Patient Index. Notification for correcting the information must be accomplished by informing the individual to whom the record pertains by mail. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations that had previously received the record about the amendment. If 38 U.S.C. 7332- protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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

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

Lighthouse Fast Healthcare Interoperability Resources API processes information electronically from its backend data source systems: VistA, MPI, CDW, HDR, and Oracle Health. Corrections/updates to a patient’s record are handled by the source systems of the information.

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 Veterans whose records contain incorrect information may not receive notification of any changes. Furthermore, incorrect information in a Veteran's record may result in improper identification.

LHFHIR API processes and transmits healthcare records including Diagnoses, Prescriptions, medications, clinical notes, etc. Unauthorized modification or destruction of health care information may result in incorrect, inappropriate, or excessively delayed treatment of patients. The system exchanges VA information between VA systems and the accuracy of the data is dependent on the source system.

Mitigation: By publishing this PIA and the PIAs of the source systems, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Virtual VA platform. Furthermore, the following source system SORNs provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

Data LHFHIR API receives from backend data sources is in read-only format, and healthcare professionals double-check its accuracy before making any decisions. In the event the data is altered, the correct data can be retrieved from the authoritative EHR sources like VistA, which minimizes adverse impacts on VA operations, assets, or individuals.

- 121VA10 / 88 FR 22112 (4/12/2023); National Patient Databases – VA AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
  - 38 U.S.C 501
- 24VA10A7 / 85 FR 62406 (10/2/2020); Patient Medical Records – VA AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
  - Title 38, United States Code, Sections 501(b) and 304
- 79VA10 / 85 FR 84114 (12/23/2020); Veteran Health Information Systems and Technology Architecture (VistA) Records – VA
- 146VA0005Q3 / 73 FR 16093 (03/26/2008); Department of Veteran's Affairs Identity Management System (VAIDMS) - VA

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 Fast Healthcare Interoperability Resources API team member. Accounts ultimately need to be approved by the System Owner before they are created. Once they do, Lighthouse adheres to project roles maintained by the VAEC mapped back to VA Active Directory groups (e.g. read-only user, project admin, etc.) depending on the employee's role.

An individual represents a consumer of the Lighthouse Fast Healthcare Interoperability Resources API. These users are subject to the onboarding requirements, follow the principles of least privilege and require approval by the System Owner before access is granted.

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

Consumers of the Lighthouse Fast Healthcare Interoperability Resources API

- Commercial Third-Party Application – These applications making use of the Lighthouse Fast Healthcare Interoperability Resources API must be granted explicit consent by the individual or have an established data sharing agreement with the VA Privacy office such as an Information Sharing Agreement (ISA) Memorandum of Understanding (MOU)

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

An individual is onboarded as a Lighthouse Fast Healthcare Interoperability Resources API team member. Accounts ultimately need to be approved by the System Owner before they are created. Once they do, Lighthouse adheres to project roles maintained by the VAEC mapped back to VA Active Directory groups (e.g. read-only user, project admin, etc.) depending on the employee's role.

Consumers of the APIs are limited to the functionality provided by the API endpoints and the permission granted to the application in use.

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

8.2b. What involvement will contractors have with the design and maintenance of the system?
Contractors are primarily responsible for the design and maintenance of the system.

8.2c. Does the contractor have a signed confidentiality agreement?

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

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

No, there is no Business Associate Agreement. 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 certificates are recorded:

- VA Privacy and Information Security Awareness and Rules of Behavior
- HIPPA Training

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

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.

For Lighthouse Fast Healthcare Interoperability Resources API staff, all employees adhere to VA-mandated trainings before accounts are provisioned to access Lighthouse Fast Healthcare Interoperability Resources API: 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. All contractors must have a public trust clearance in place to access the system and PII. The need for VA contractors to access PII is limited to investigations of any issues that arise that prevent the API from working as designed.

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

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

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

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

8.4a If Yes, provide:

1. *The Security Plan Status:* SDE Survey Complete
2. *The System Security Plan Status Date:* Initial Completion: 4/27/23. Most recent update: 8/2/24.

3. *The Authorization Status:* cATO Status – Continuous RMF
4. *The Authorization Date:* Round 2 Issued on 2/22/24.
5. *The Authorization Termination Date:* Continuous cATO
6. *The Risk Review Completion Date:* Clinical Health API: 3/18/24. Patient Health API: 8/7/24.
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.***

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 Fast Healthcare Interoperability Resources API is middleware Software as a Service (SaaS) 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.*

The Lighthouse Fast Healthcare Interoperability Resources API system does not own or store data. The electronic health record (EHR) data that the LHFHIR API provides to consumers is VA owned data.

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

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

This question is related to privacy control DI-1, Data Quality.

The cloud service provider will not collect any ancillary data.

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

System data is not held by the cloud provider. The contractors designing and maintaining the system hold the responsibility to protect the data. The cloud provider may hold logs of calls made to the LHFHIR API.

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

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

The Lighthouse Fast Healthcare Interoperability Resources API system does not use Robotic Process Automation.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2025.01.15 14:33:10 -06'00'

Privacy Officer, Gina Siefert

JEFFREY GARDINER Digitally signed by JEFFREY GARDINER
Date: 2025.01.16 07:27:23 -05'00'

Information System Security Officer, Jeffrey Scott Gardiner

ANDREW FICHTER Digitally signed by ANDREW FICHTER
Date: 2025.01.16 12:09:35 -05'00'

Information System 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).

Lighthouse Fast Healthcare Interoperability Resources API does not collect PII information. LFHIR API defers collection notification to its data source systems. Privacy Notice is served by the data source system at time of collection and/or through the data source systems' PIAs and SORNs.

- 121VA10 / 88 FR 22112 (4/12/2023); National Patient Databases – VA AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
  - 38 U.S.C 501
- 24VA10A7 / 85 FR 62406 (10/2/2020); Patient Medical Records – VA AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
  - Title 38, United States Code, Sections 501(b) and 304
- 79VA10 / 85 FR 84114 (12/23/2020); Veteran Health Information Systems and Technology Architecture (VistA) Records – VA
- 146VA0005Q3 / 73 FR 16093 (03/26/2008); Department of Veteran's Affairs Identity Management System (VAIDMS) - VA

For third-party applications that use Lighthouse Fast Healthcare Interoperability Resources API, the users are prompted to provide revokable consent for information requested by the consumer application. Checkboxes appear beside each of the following data elements to allow users to choose their data they want to allow access to share.

☐ **VA Patient ID**
Your VA Patient ID (also called Integration Control Number or ICN) links your VA medical info to you. This is not your social security number.

☐ **Demographic information**
Information about you, such as your name, birth date, address, and more.

☐ **Allergies**
A list of any substances to which you have a negative reaction. Examples include pollen, gluten, or bee stings.

☐ **Health conditions and diagnoses**
A list of any conditions that impact your health. Examples include diabetes or being overweight.

☐ **Test results**
Examples are lab results, x-ray or MRI results, or pregnancy tests.

☐ **Vaccines**
A list of your vaccines and immunizations.

☐ **Medication information**
Lists ingredients in your medication and shows the medication's package information.

☐ **Prescriptions**
All of your prescriptions. Examples include prescription medications, aspirin, vitamins, or eyeglasses.

☐ **Medication list**
All medications you are currently taking, as reported by you or your doctor.

☐ **Health data**
Any data about you, such as smoking status, blood pressure, laboratory results, and more. These items are not always health issues, but they may be.

☐ **Surgeries**
Any surgeries that required you to stay in a hospital overnight.

☐ **Prescribed medications and instructions**
Lists all the medications you are prescribed, whether they are over the counter or not, and the instructions for how to use them. This is like what is included for prescriptions but does not include non-medical items like eyeglasses.

☐ **Healthcare staff**
Names and related data, such as work addresses, for anyone who is professionally involved with making sure you get health care. Examples include doctors, therapists, receptionists, or service dogs.

☐ **Staff roles**
The locations and kinds of services that your healthcare staff are licensed or qualified to provide.

☐ **Organization**
The organizations, groups, or companies involved in your care.

☐ **Devices and supplies**
Items used to provide you with health care. These may be medical or non-medical. Examples include monitors or walkers.

☐ **Location of service or resource**
The location where a service or an event took place or where an item is stored.

☐ **Appointments**

A single healthcare appointment in the past or future which may be in-person, virtual, or part of a series. Examples are an office visit, a call between doctors, or a reservation for x-rays.

☐ **Encounters**
Gives information about a patient's visit with a healthcare provider. It tells about the location of the visit and the kinds of services that happened. Encounters may have already occurred or may be scheduled for the future.

☐ **Device Request**
A request for a patient to use a medical device. This device could be an implantable device or an external assistive device.

☐ **Binary**
The content of documents that details the care activities of a patient. This includes notes that provide transitions of care, care planning, quality reporting, billing, and even handwritten notes by providers.

☐ **Document Reference**
Provides metadata on documents that detail the care activities of a patient. Metadata include a document's type, date, location, and author.

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)