Privacy Impact Assessment for the VA IT System called:

Lighthouse Fast Healthcare Interoperability Resources API

Veterans Affairs Central Office (VACO)

Product Engineering

Date PIA submitted for review:

08/22/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lynn Olkowski	Lynn.Olkowski@va.gov	202-632-8405
Information System Security Officer (ISSO)	Andrew Vilailack	Andrew.Vilailack@va.gov	813-970-7568
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?" and will be published online to accompany the PIA link.

The Lighthouse Fast Healthcare Interoperability Resources API (LHFHIR) 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 consumers. 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 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. The IT system name and the name of the program office that owns the IT system.

IT System:

Lighthouse Fast Healthcare Interoperability Resources API – Program Office: Product Engineering

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

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

C. Indicate the ownership or control of the IT system or project.

VA Owned and Operated.

2. Information Collection and Sharing

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

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

E. A general description of the information in the IT system and the purpose for collecting this information.

LHFHIR provides access to the VA EHR and Healthcare related data including: Patient Identifiers, Patient Demographic information, Allergies, Health Conditions and Diagnoses, Medical test results, vaccinations, medication details, prescriptions, self-reported medications, surgeries, medical devices, appointments, medical visits, clinical notes and other health data 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.

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.

The Lighthouse Fast Healthcare Interoperability Resources API provides read-only access to the VA EHR data which includes Patient Identifiers, Patient Demographic information, Allergies, Health Conditions and Diagnoses, Medical test results, vaccinations, medication details, prescriptions, self-reported medications, surgeries, medical devices, appointments, medical visits, clinical notes and other health data. This data is sourced from VA sources such as Corporate Data Warehouse, VistA, Health Data Repository and Master Patient Index and is shared with authorized third-party commercial applications based on direct consent of individuals or established data sharing agreements with the VA and in compliance with the ONC 21st Century Cures Act, as well as, other authorized internal VA applications which needs access to the medical record data to authorized users such as clinicians.

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

The system will only be hosted at one site, the VA-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

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

The legal authorities to operate the system are: 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 939. Also the following VA System of Record Notices (SORNs) apply to the Lighthouse Fast Healthcare Interoperability Resources API : · National Patient Databases – VA, SORN 121VA10A7 / 83 FR 6094 · Patient Medical Records – VA, SORN 24VA10A7 / 85 FR 62406 · Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 / 85 FR 84114

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The system is in the process of being modified being split from the Digital Veteran Platform (DVP) (VASI# 2196) and added as an independent system as a tenant of the Lighthouse Delivery Infrastructure (LHDI) (VASI# 2890) and the SORNs are not in need of revision. The SORNs do cover cloud usage.

D. System Changes

J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*

The completion of this PIA will not result in circumstances that require changes to business processes

K. *Whether the completion of this PIA could potentially result in technology changes*

The completion of this PIA will not result in technology changes

Section 1. Characterization of the Information

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

1.1 What information is collected, used, disseminated, created, or maintained in the system?

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

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

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

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
☒ 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*
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☒ Gender
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☒ Next of Kin
☒ Other Data Elements (list below)

- Electronic Data Interchange Personal Identifier (EDIPI)
- Business Organization
- Business Phone Number
- National Provider Identifier (NPI)
- Covid-19 Vaccinations
- Surgeries
- Medical Devices
- Allergies – Substances to which person had a negative reaction

PII Mapping of Components (Servers/Database)

Lighthouse Fast Healthcare Interoperability Resources API consists of zero key components (databases). 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	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
NA	NA	NA	NA	NA	NA

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

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

The Lighthouse Fast Healthcare Interoperability Resources API does not store data nor does it collect any data from individuals. The system provides application programming interfaces to VA sources of this data such as the Corporate Data Warehouse, VistA EHR instances, Health Data Repository, and/or Master Person Index. The Lighthouse Fast Healthcare Interoperability Resources API access data from these systems and presents the information to the authorized consumers of the API using the 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.

The Lighthouse Fast Healthcare Interoperability Resources API serves the 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 If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

The Lighthouse Fast Healthcare Interoperability Resources API does not create information.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

The Lighthouse Fast Healthcare Interoperability Resources API access information from other VA systems such as Corporate Data Warehouse through database connections, VistA instances through direct VistALink connections, Health Data Repository through SOAP APIs and Master Patient Index through SOAP APIs. Information processed will be safeguarded in accordance to 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, give 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 How will the information be checked for accuracy? How often will it be checked?

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

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

The Lighthouse Fast Healthcare Interoperability Resources API is not storing information directly. The integrity of the data is based on the integrity controls in place from where the information is requested. All the information will be checked at the source end. Information collected and processed will be safeguarded in accordance to VA Handbook 6500 and FIPS 140-2 encryption and data processing standards

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

The 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 What specific legal authorities, arrangements, and agreements defined the collection of information?

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

The legal authorities to operate the system are 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 939. Also the following VA System of Record Notices (SORNs) apply to the Lighthouse Fast Healthcare Interoperability Resources API : · National Patient Databases – VA, SORN 121VA10A7 / 83 FR 6094 · Patient Medical Records – VA, SORN 24VA10A7 / 85 FR 62406 · Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 / 85 FR 84114

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

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

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

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

<u>Principle of Data Quality and Integrity:</u> Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: Lighthouse Fast Healthcare Interoperability Resources APIs processes Personally Identifiable Information (PII) and Personal Health Information (PHI) which can be used to identify a Veteran, VA Patient or individual. If this information is breached or disclosed inappropriately then this could result personal or financial harm to the individual whose data was exposed and provide a negative impact on the VA.

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. All systems and individual with access to the system will be approved, authorized, and authenticated before access is granted by VA Project Manager and System Owner. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors. LHFHIR makes use of OAuth 2.0 and uses the principle of privilege for granting access to the endpoints and data.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system 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.

All data processed is returned to the approved Lighthouse Fast Healthcare Interoperability Resources API consumer (third-party or internal VA application for use. The data is transiently passed through the Lighthouse Fast Healthcare Interoperability Resources API from backend data sources to these consumers and is protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards
Name: Demographic information returned about the Patient. Used to identify a Patient
Social Security Number: Demographic information returned about the Patient.
Date of Birth: Demographic Information returned about the Patient. Used to identify a Patient.
Mother's Maiden Name: Demographic Information returned about the Patient. Used to identify a Patient.
Personal Mailing Address: Demographic Information returned about the Patient. Used to identify a Patient.
Personal Phone Number: Demographic Information returned about the Patient
Person Fax Number: Demographic Information returned about the Patient.
Personal Email Address: Demographic Information returned about the Patient.
Emergency Contact Information: Demographic Information returned about the Patient.
Medication: Returned as part of the medical record.
Medical Records: Returned medical data for the patient and/or authorized clinician to view

Race/Ethnicity: Demographic Information returned about the Patient.
Medical Record Number: Used to identify a Patient
Gender: Demographic Information returned about the Patient. Used to identify a Patient.
Integrated Control Number: Used to identify a Patient
Next of Kin: Demographic Information returned about the Patient.
Electronic Data Interchange Personal Identifier: Used to identify a Patient
Business Organization: Used to share what organization a Practitioner is a part of.
Business Phone Numbers: Used to share how to contact and organization or Practitioner
Covid-19 Vaccinations: Data returned as part of the medical record.
Surgeries: Data returned as part of the medical record.
Medical Devices: Data returned as part of the medical record.
Allergies: Data returned as part of the medical record.

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

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

Lighthouse Fast Healthcare Interoperability Resources API are middleware and does not create information itself. It exchanges information between internal VA system and approved (by VA Product Engineering) third-party and internal VA API consumers. Lighthouse Fast Healthcare Interoperability Resources API does not analyze any data passing through for accuracy. The information exchanged in the Lighthouse Fast Healthcare Interoperability Resources API may contain PII and PHI. The only transformations of data performed are to align the data to the Health Level Seven 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 the Lighthouse Fast Healthcare Interoperability Resources API do not provide or replace the consultation, guidance, or care of a health professional or other qualified provider. Health care 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.

The Lighthouse Fast Healthcare Interoperability Resources API do not create any new information.

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

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

Data in encrypted in transit (TLS 1.2+) and uses authenticated access (i.e. API Keys and OAuth 2.0 access tokens). There is no data at rest.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

No additional SSN protections are in place beyond being encrypted in transit using FIPS 140-2 compliant algorithms

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

The Lighthouse Fast Healthcare Interoperability Resources API run entirely in the VAEC AWS cloud and therefore satisfy 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. ***<u>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.</u>***

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 consumers the individual is requesting access to

their data via the application that integrates with the Lighthouse Fast Healthcare Interoperability Resources API and must be provided the ability to revoke consent at any time. Alternatively, the third-party consumer may be accessing data based on 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?

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

2.4c Does access require manager approval?

Yes System Owner approval is required for access.

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

Yes there are logs for each access of the APIs

2.4e Who is responsible for assuring safeguards for the PII?

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? This question is related to privacy control DM-2, Data Retention and Disposal.*

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

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA Records Officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
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/PHI.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: Lighthouse Fast Healthcare Interoperability Resources APIs processes Personally Identifiable Information (PII) and Personal Health Information (PHI) which can be used to identify a Veteran, VA Patient or individual. If this information is breached or disclosed inappropriately then this could result personal or financial harm to the individual whose data was exposed and provide a negative impact on the VA

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. All systems and individual with access to the system will be approved,

authorized, and authenticated before access is granted by VA Project Manager and System Owner. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors. LHFHIR makes use of OAuth 2.0 and uses the principle of privilege for granting access to the endpoints and data.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veteran Health Administration (VHA)	Source of Information for the APIs	Personally Identifiable Information (PII), Protected Health Information (PHI),	SQL Server Connection (Windows authentication/Kerberos

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Corporate Data Warehouse (CDW)		and Individually Identifiable Information (III) as defined in HL7 FHIR including implementation Guides (Argonaut Data Query, US Core, HL7 Da Vinci PDex Plan Net). This includes patient name, sex, date of birth, race, ethnicity, preferred language, smoking status, problems, medications, medication allergies, laboratory test(s), laboratory value(s)/result(s), vital signs, procedures, immunizations, health concerns, clinical notes. devices, visits, and appointments. Other information is also extracted such as Nutrition, Podiatry, and Dentistry service availability lookup in VA clinics	
Office of Information and Technology (OI&T) Master Person Index	Uniquely identify users and access correlated identifiers for the person	Personally Identifiable Information (PII) and Individually Identifiable Information (III). This includes identify traits such as full name, social security number, EDIPI, file number, and date of birth	PII/III processed electronically through encryption via APIs
Veterans Health Administration (VHA) Health Data Repository (HDR)	Access clinical notes to be served by the APIs	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) related to read-only patient clinical data. This includes allergies, discharge summary,	PII/PHI/III processed electronically through encryption via API

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		consultations, flags, laboratory results, medications, notes, orders, problems, radiology, exams, visits, vitals, additional signers, appointments, patient remarks, sensitive patient, VistA users	
Veterans Health Administration (VHA) Veteran Health Information Systems and Technology (VistA)	Access to the Electronic Health Record (EHR) data	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III). This includes patient vital signs, lab results, ICN, and demographics.	PII/PHI/III processed electronically through encryption via API

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

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

Mitigation: The principle of need-to-know is strictly adhered to for the Lighthouse Fast Healthcare Interoperability Resources API staff. Only support staff with a clear business purpose are allowed access to the system and the information processed therein.

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 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, 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 External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit***	***List the method of transmission and the measures in place to secure data***

			external sharing (can be more than one)	
Multiple *Approved (by VA Product Engineering) third-party API consumer	The data is shared to be in compliance with the ONC 21st Century Cures Act. VA Patients can view their VA Medical Records through approved third-party applications. Internal VA Applications can access a Patient's medical record in accordance with industry standards for interoperability .	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III). Depending on the API accessed, the list of data elements varies. This may include full name, date of birth, social security number, enrollment and eligibility, and benefits claims forms, but can vary based on the API.	National ISA/ MOU CRADA VA API Terms of Service (ToS) / Code of Conduct (CoC)	API Keys OAuth 2.0 Access Tokens Data is encrypted in transit (TLS 1.2+)

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.

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

Follow the format below:

Privacy Risk: The privacy risk associated with sharing data outside of the Department of Veteran's Affairs is that data may be disclosed to individuals who do not have access and heightens the threat of misuse.

Mitigation: Lighthouse Fast Healthcare Interoperability Resources API follows the principle of need-to-know strictly. Only support staff with a clear business purpose are allowed access to the data processed therein. Connections are encrypted in transit via SSL across our Network Services Operations Center (NSOC)-monitored site-to-site VPN connections. API consumer connections are encrypted in transit and agrees to the VA API Terms of Service (ToS) / Code of Conduct (CoC) while also being subject to an approval process involving the System Owner. Access controls are in place as dictated by VA's Risk Management Framework process, following required VA Handbook 6500 and NIST Guidelines. Audit log information is forwarded to the Cybersecurity Operations Center (CSOC) for continuous review and monitoring via installed agents by the VA Enterprise Cloud. Lighthouse Fast Healthcare Interoperability Resources API also has continuous monitoring and alerting in place to detect traffic anomalies and malicious attempts to gain unauthorized access.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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 This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Lighthouse Fast Healthcare Interoperability Resources API does not collect PII information. It sources VA Patient medical record information from sources within the VA such as Corporate Data Warehouse, VistA, Health Data Repository, and MPI and passes this information through to authorized consumers. 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 applications Terms Of Service and Privacy Policy. For application that are not attended by the users a documented agreement such

as an ISA/MOU and/or a CRADA are established. This Privacy Impact Assessment (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 the 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. If it was provided, attach a copy of the current notice.

Notice is provided as part of the privacy policy of the consumers of the API and are prompted to provide revokable consent.

This Privacy Impact Assessment (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 the agencies. VA System of Record Notices (SORNs) which are published in the Federal Register and available online

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

VA System of Record Notices (SORNs) which are published in the Federal Register and available online National Patient Databases –VA, SORN 121VA10A7 / 83 FR 6094 (Link)
Patient Medical Records – VA, SORN 24VA10A7 / 85 FR 62406 (Link)
Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 / 85 FR 84114 (Link)

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 to 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, 2017 1.575(a)). Individuals do have an opportunity to decline to provide information at any time. No, there is not a penalty or denial of service for declining to provide 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 Form10-5345) describing what information is to be sent out and to whom it is being sent to. Patients have the right to opt-out of VA facility directories. VHA Directive 1605.1 section 5 "Individual's Rights" lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. 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.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to 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 Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation: The Lighthouse Fast Healthcare Interoperability Resources API mitigates this risk by ensuring that individuals are provided notice of information processing and notice of the system's existence.

Section 7. Access, Redress, and Correction

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

7.1 What are the procedures that allow individuals to gain access to their information?

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

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

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).

N/A – LHFHIR is not exempt from 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.

N/A – LHFHIR 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 Fast Healthcare Interoperability Resources API is an API 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.

The 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.

The Lighthouse Fast Healthcare Interoperability Resources API process information electronically from the systems noted in Sections 4 and 5. Corrections/updates 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 System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his 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.

Mitigation: By publishing this PIA 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 SORN provides the point of contact for members of the public who have questions or concerns about applications and evidence files.

The following SORNs are applicable to Lighthouse Fast Healthcare Interoperability Resources API:

National Patient Databases –VA, SORN 121VA10A7 / 83 FR 6094 (Link)
Patient Medical Records – VA, SORN 24VA10A7 / 85 FR 62406 (Link)
Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 / 85 FR 84114 (Link)

Section 8. Technical Access and Security

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

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

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

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

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.

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

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

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.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Please provide response here
2. *The System Security Plan Status Date:* Please provide response here
3. *The Authorization Status:* Please provide response here
4. *The Authorization Date:* Please provide response here
5. *The Authorization Termination Date:* Please provide response here
6. *The Risk Review Completion Date:* Please provide response here

7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Please provide response 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 No or In Process, provide your ***Initial Operating Capability (IOC) date.***

No. estimated date is 9/4/2023

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.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Lighthouse Fast Healthcare Interoperability Resources API is middleware 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 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 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

Lighthouse Fast Healthcare Interoperability Resources API is hosted in VAEC AWS and is covered under the AWS Enterprise Contract. The VAEC and System Owner are ultimately accountable for the security and privacy of data held by a cloud provider. All data will be processed through the

VAEC AWS GovCloud environment. This is part of the Shared Responsibility Model for Security in the Cloud

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.

This is governed by the Shared Responsibility Model for Security in the Cloud. The Lighthouse Fast Healthcare Interoperability Resources API is responsible for its data. For all cloud deployment types, the customer owns their data and identities. The customer is responsible for protecting the security of its data and identities, and the cloud components it controls (which varies by service type)

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).

No Robotics Process Automation is used.

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**

ID	Privacy Controls
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.

Lynn A Olkowski

Digitally signed by Lynn A Olkowski
Date: 2023.09.05 13:25:59 -05'00'

Privacy Officer, Lynn Olkowski

ANDREW VILAILACK

Digitally signed by ANDREW VILAILACK
Date: 2023.09.05 15:03:08 -04'00'

Information System Security Officer, Andrew Vilailack

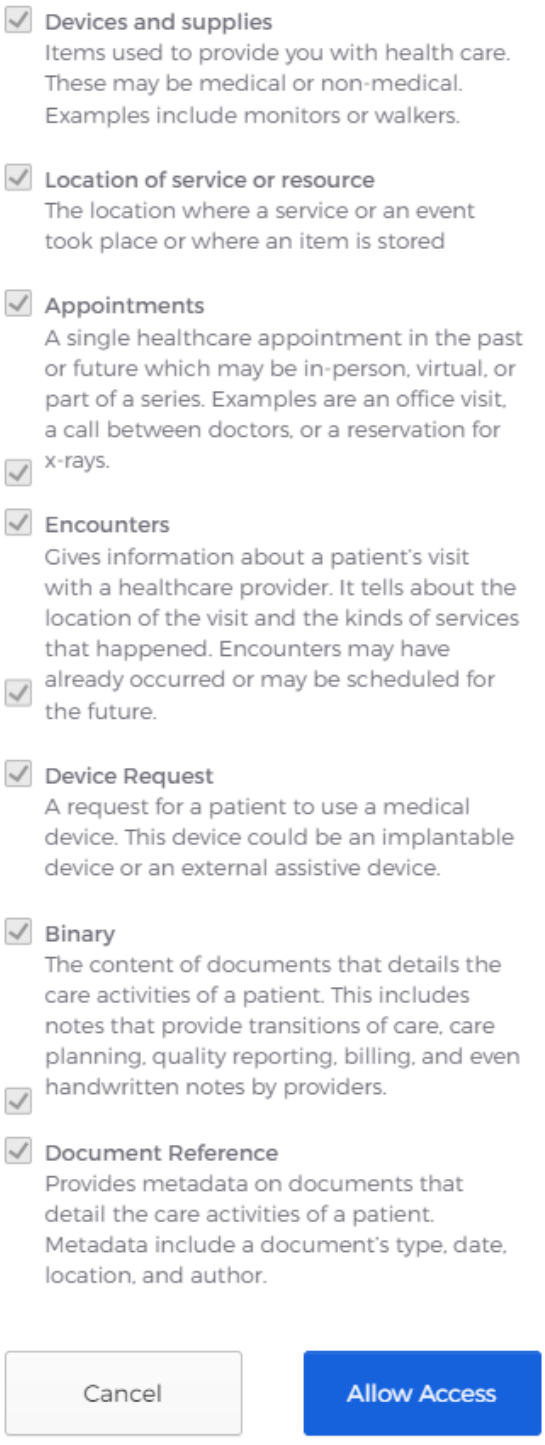
ANDREW FICHTER

Digitally signed by ANDREW FICHTER
Date: 2023.09.05 15:48:51 -04'00'

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).



HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices