Privacy Impact Assessment for the VA IT System called:

VA Light Electronic Action Framework Cloud Assessing (LEAF)

Office of Information and Technology (OIT), Franchise Budget Office, Veterans Affairs Central Office (VACO)

Date PIA submitted for review:

July 28, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lynn A Olkowski	Lynn.Olkowski@va.gov	202-632-8405
Information System Security Officer (ISSO)	Rustine Johnson	Rustine.Johnson@va.gov	414-584-2000 x42194
Information System Owner	Michael Gao	Michael.Gao@va.gov	919-695-3426

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

The Light Electronic Action Framework (LEAF) is a government-off-the-shelf (GOTS) platform for digitizing multilayered, time-consuming processes. Built by VA for VA, it empowers non-technical users to implement workflows and digital forms that allow for faster turnaround, complete transparency, national standardization, and status tracking.

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.*

VA Light Electronic Action Framework (LEAF). Office of Information and Technology (OIT), Franchise Budget Office, Veterans Affairs Central Office (VACO)

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

LEAF is a business process management platform that provides rapid development and deployment capabilities that are scalable and cost-effective to help deliver world-class service to Veterans.

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

Department of Veterans Affairs

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.*

Approximately 450,000 individuals. A typical individual is directly involved in one or more business processes operated by VA.

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

Information being collected in LEAF is dependent on the individual process requirements. This information serves to provide necessary information to resolve workflows. The following examples illustrate the varied workflows implemented within the LEAF platform.

For example, in a travel approval workflow, the system may collect the traveler's name, contract information, and financial information to determine travel cost and compensation.

In a Clinic Profile Management workflow, the system may collect names of individuals working in a particular clinic to provide notification of scheduling changes.

In a Power of Attorney workflow, the system may collect Personally Identifiable Information of individuals to assist with the onboarding of individuals who have requested access to Veteran Benefits Administration Information Systems.

In a Vaccination Status Report workflow, the system may collect names of VA employees and/or contractors, dates of vaccination, location of vaccination, to verify vaccination and assist VA in prioritizing deployment of personal protective equipment and minimizing the spread of communicable diseases.

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

LEAF does not directly share information with other VA systems, however individual implementations may elect to automatically download data to a separate database.

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.

There are over 4,000 active implementations of LEAF, however consistency is achieved by utilizing the same "need to know" LEAF security feature across all sites. This feature limits information access to individuals who are involved in the specific workflow.

3. Legal Authority and SORN

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

Title 38, United States Code, Section 501

(https://www.oprm.va.gov/privacy/systems_of_records.aspx).

01VA022 - Accreditation Records-VA
https://www.oprm.va.gov/docs/sorn/SORN01VA22.PDF

150VA19 -Administrative Data Repository-VA
https://www.govinfo.gov/content/pkg/FR-2008-11-26/pdf/E8-28183.pdf

Employee Medical File System of Records (Title 38)-VA:
Published Prior to 1995, 08VA05

OPM/GOVT-1: General Personnel Records
December 11, 2012, 77 FR 79694; modification published November 30, 2015, 80 FR 74815

General Personnel Records (Title 38)-VA
July 20, 2000, 65 FR 45131

103VA07B – Police and Security Records-VA
Federal Register, Volume 87, No. 203 (Friday, October 21, 2022)

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?*

N/A for the first question.

Yes,The VA Profile system maintains records in a system known as the VA Profile Data Repository (VA PROFILEDB) hosted in a containerized environment at a federally rated FISMA moderate data center at the Austin Information Technology Center (AITC), located at 1615 East Woodward Street, Austin, Texas 78772. Capabilities implemented in FY2020 and later will be hosted in the FISMA-high VA Enterprise Cloud (VAEC).

D. System Changes

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

N/A

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

N/A

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)

OIG Investigation Findings, Vehicle Insurance Policy Numbers

*Occupational License Number

PII Mapping of Components (Servers/Database)

VA Leaf (Cloud) Assessing consists of 2 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VA Leaf (Cloud) Assessing 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.

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
Web Application	Yes	No	See section 1.1 for complete list	Required to resolve business processes. Examples have been given in the system overview.	Encryption in transit, Session Timeout, Masked Fields, Two-factor authentication
Database	Yes	Yes	See section	Required to resolve business	Encryption in transit,

			1.1 for complete list	processes. Examples have been given in the system overview.	Encryption at rest, Virtual Private Network

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?

Information is collected directly from the individual. In workflows where an individual has an active VA network account, the information is imported from the VA Global Address List.

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 information used from the VA Global Address List is required to eliminate the possibility of typos when interacting with email addresses or user account names.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

LEAF can present information in a report, when initiated by an authorized individual user.

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?

Information is collected by input from authorized users or routines, through an electronic form, designed by administrators, and presented by the system.

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.

N/A, The type of information collected is variable, depending on the individual business process being implemented by an authorized VA employee or contractor.

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.

Information is checked for accuracy depending on the specific workflow being implemented. Typically, the lifecycle of information is very short, as after information is used as part of a work duty, it is no-longer needed. To prevent and mitigate data corruption, LEAF utilizes technology that provides 99.999999999% data durability, and cryptography provides pass/fail assurance.

Individual instance data accuracy validation is required by the instance owner to ensure accuracy and integrity of data being used for their specific business purpose.

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.

N/A

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 Secretary of the VA has authority to prescribe all rules and regulations which are necessary or appropriate to carry out the laws administered by the department. Title 38, United States Code, Section 501

VA Handbook 6500 requires an information system to be authorized through an Authorization to Operate (ATO).

VA Leaf (Cloud) Assessing maintains an approved ATO, which are reviewed on a scheduled basis. As of this writing, the most recent ATO was granted on February 17, 2022 and will be reviewed before February 17, 2025

(https://www.oprm.va.gov/privacy/systems_of_records.aspx).
01VA022 - Accreditation Records-VA
https://www.oprm.va.gov/docs/sorn/SORN01VA22.PDF

150VA19 -Administrative Data Repository-VA
https://www.govinfo.gov/content/pkg/FR-2008-11-26/pdf/E8-28183.pdf

Employee Medical File System of Records (Title 38)-VA:
Published Prior to 1995, 08VA05

OPM/GOVT-1: General Personnel Records
December 11, 2012, 77 FR 79694; modification published November 30, 2015, 80 FR 74815

General Personnel Records (Title 38)-VA
July 20, 2000, 65 FR 45131

103VA07B – Police and Security Records-VA
Federal Register, Volume 87, No. 203 (Friday, October 21, 2022)

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

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

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

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

<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:

<u>Privacy Risk:</u> LEAF supports the mission of VA by providing a secure mechanism for VA employees and contractors to implement a variety of business processes within VA. Broad use of LEAF presents a risk as policies may be inconsistently applied for all individual implementations.

<u>Mitigation:</u> VA maintains policies and procedures to protect business practices implemented within LEAF, and LEAF implements security features to limit and monitor data access to authorized individuals..
To mitigate the risk of inconsistently secure implementations, procedural and technical solutions have been implemented. Procedures such as annual training and information security exercises are required for all VA network account holders. LEAF additionally uses system level controls, automatically applied to all individual LEAF sites, to inform compliance status and consistently applies technical solutions such as access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, physical and environmental protection, system information integrity, security assessment, incident response, encryption in transit, Session Timeout, Masked Fields, and Two-factor authentication.

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.

As covered within examples listed in the system overview, LEAF helps modernize business processes by reducing manual, labor-intensive steps in workflows. Information used in the system is utilized to fulfill workflows that have been implemented in LEAF.

Regarding each use:

The uses cases vary depending on the personnel that are utilizing LEAF.

Information being collected in LEAF is dependent on the individual process requirements. This information serves to provide necessary information to resolve workflows. The following examples illustrate the varied workflows implemented within the LEAF platform.
For example, in a travel approval workflow, the system may collect the traveler's name, contract information, and financial information to determine travel cost and compensation.
In a Clinic Profile Management workflow, the system may collect names of individuals working in a particular clinic to provide notification of scheduling changes.
In a Power of Attorney workflow, the system may collect Personally Identifiable Information of individuals to assist with the onboarding of individuals who have requested access to Veteran Benefits Administration Information Systems.
In a Vaccination Status Report workflow, the system may collect names of VA employees and/or contractors, dates of vaccination, location of vaccination, to verify vaccination and assist VA in prioritizing deployment of personal protective equipment and minimizing the spread of communicable diseases.

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.

LEAF does not analyze data. LEAF generates data exports of the data in electronic formats including CSV, JSON, XML.

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.

Records within LEAF are newly created for each business transaction, and information is made available to VA employees/contractors to conduct VA business.

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?

LEAF utilizes Encryption in transit, Encryption at rest, Session Timeout, Masked Fields, Two-factor authentication, and Virtual Private Network to protect data in transit and at rest.

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

PHI/PII fields are marked as sensitive. System enforces privacy protections in the user interface by hiding data until an explicit action is taken to reveal it.

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

LEAF is implemented by complying with VA Information Security Rules of Behavior, and complying with OIT policies on use of two-factor authentication. LEAF also provides a "need to know" feature to protect the confidentiality of records, which limits data access to individuals who have a defined role in an implemented business process.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

The LEAF-S Certification process guides site administrators through the establishment of need-to-know access to PII data, and site administrators are responsible for reviewing and safeguarding the data. This process includes a Supervisory review and Privacy Officer approval step. All access is monitored and recorded through web server logs, which includes every transaction made. All data is stored encrypted at rest using technology provided by the VA Enterprise Cloud. All data is transmitted using TLS encryption. VA OIT maintains security procedures when granting GAL access and PIV badges, as this access is a prerequisite for using LEAF.

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

Access for individual business processes are documented in LEAF's Workflow and Form components.

2.4c Does access require manager approval?

Yes

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

All transactions are logged.

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

The LEAF Technical Director

Section 3. Retention of Information

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

3.1 What information is retained?

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

Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Phone Numbers, Personal Fax Numbers, Personal Email Address, Emergency Contact Information, Financial Information, Occupational License Numbers, Vehicle License Plate Number, Internet Protocol Address Numbers, Medications, Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Gender, Integrated Control Number, Military History/Service Connection, Next of Kin, OIT Investigation Findings.

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.*

Information is retained with respect to the individual business process implemented within LEAF. An Administrator or Records Manager may configure this to be between one and thirty years.

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?

At the time of this writing, the control interface in LEAF is limited to manual identification of retention schedules, by associating individually implemented processes with The General Records Schedules published by NARA.

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

General Records Schedule - Occupational individual medical case files. DAA-GRS2017-0010- 0009 – NARA approved to destroy 30 years after employee separation.

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

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.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), https://www.va.gov/vapubs. When required, this data is deleted from their file location and then permanently deleted from the deleted items, or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1. Additionally, this system follows Field Security Service (FSS) Bulletin

#176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

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.

Data collected in LEAF is not used for research, testing or training new applications or information systems. LEAF utilizes randomly generated names, placeholders, and conducts testing in a computing environment segregated from real data.

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: There is a risk that the information maintained by LEAF will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released.

Mitigation: Collecting and retaining only information necessary for fulfilling the VA mission. This ensures that data is held for only as long as necessary. Users refer to the VA Archive policies and procedures to protect this business practice date and should be purging records according to the appropriate schedules. Least privilege concepts are used where only LEAF authorized administrators and/or those authorized by LEAF administrations are given the capability to run reports which may contain large information sets.

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***
Office of Information and Technology, VA	Promote the health and safety of the Federal workforce	Numbers, Personal Fax Numbers, Personal Email Address, Emergency Contact	Secure database connection using

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	and efficiency of the civil service	Information, Financial Information, Occupational License Numbers, Vehicle License Plate Number, Internet Protocol Address Numbers, Medications, Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Gender, Integrated Control Number, Military History/Service Connection, Next of Kin, OIT Investigation Findings	Microsoft SQL Server protocols

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: Information may be accessed by unauthorized individuals, or information may be shared with unauthorized individuals.

Mitigation: LEAF is only accessible from the VA intranet, which requires two-factor authentication. An individual must first have a VA Network account assigned by the VA Office of Information Technology to initially log into the system.
Once logged in, site administrators establish access to data by assigning role based access to their business process workflow. Session timeouts are also utilized to automatically log out unattended sessions.
The criteria for access to PII data is established by the Site Administrator, Supervisor, and Privacy Officer, and further secured through the “need to know” data access feature within LEAF.

Access to the VA network is governed by policies that require annual training to reinforce that information may only be shared with people who have a bona fide business need.

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***	***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 external sharing***	***List the method of transmission and the measures in place to secure data***

	office or IT system		***(can be more than one)***	
N/A	N/A	N/A	N/A	N/A

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.

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> N/A – LEAF does not share/receive with external organizations.

<u>Mitigation:</u> N/A

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.

Federal Register /Vol. 73, No. 229
Administrative Data Repository – VA
OPM/GOVT-1: General Personnel Records: *December 11, 2012, 77 FR 79694; modification published November 30, 2015, 80 FR 74815*

General Personnel Records (Title 38)-VA: *July 20, 2000, 65 FR 45131*

OPM/GOVT-10: Employee Medical File System Records: *June 21, 2010, 75 FR 35099; modification published November 30,2015, 80 FR 74815*

Employee Medical File System of Records (Title 38)-VA: Employee Medical File System of Records (Title 38)-VA: *Published Prior to 1995, 08VA05*

01VA022 - Accreditation Records-VA Federal Register, Volume 78 Issue 245 (Friday, December 20, 2013) (govinfo.gov)

150VA19 – Administrative Data Repository-VA Federal Register, Volume 73, No. 229 (Wednesday, November 26, 2008)

103VA07B – Police and Security Records-VA Federal Register, Volume 87, No. 203 (Friday, October 21, 2022)

https://www.oprm.va.gov/privacy/systems_of_records.aspx

Additional Privacy Act Notices may be implemented for individual business processes. An example of one used has been added to Appendix A.

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

N/A
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.

Individual processes may present notices differently within LEAF. Processes which are novel and not routine may provide notice within the application. See Appendix A for example.

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.

VA permits individuals to give consent or agree to the collection or use of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. If individuals are not willing to give information verbally then they are not required to do so. Individuals are made aware of when they must give consent when there is data collected about them through the VA Notice of Privacy Practices and conversations with VA employees. VA Forms are reviewed by VA Central Office periodically to ensure compliance with various requirements including that Privacy Act Statements which are on forms that collect personal information from Veterans or individuals. VA uses PII and PHI only as legally permitted including obtaining authorizations were required. If the individual does not want to give consent then they are not required to in most cases unless there is a statute or regulation that requests the collecting and then consent is not necessary but when legally required VA obtains a specifically signed written authorization for each intended purpose from individuals prior to releasing, disclosing or sharing PII and PHI.
Link to Notice of VA Privacy Policies here:
https://www.oprm.va.gov/privacy/resources_privacy.aspx

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.

If an individual does not consent to particular uses of their information, they may contact the local LEAF administrator to specify how information may be used.

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

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

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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 an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practices (NOPP) to employees when they receive care and Veterans when they apply for benefits. The VA also mitigates this risk by providing the public with two forms of notice as discussed in detail in question 6.1, including the Privacy Impact Analysis and the System of Record Notice. Individuals seeking information regarding access to and contesting of VA medical records may write, call, or visit the last VA facility where medical care was provided

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.***

The VHA Notice of Privacy Practices informs Veterans of their right to obtain copies of their PII maintained in VHA records. Each VHA Privacy Act system of records notice (SORN) informs individuals how to obtain access to records maintained on them in the SORN. VHA permits individual to obtain access to or get copies of their PII, and this is outlined in VHA policy such as VHA Directive 1605.01 Privacy and Release of Information. Individuals must provide a written request for copies of their records to the VHA facility Privacy Officer for medical records or the System Manager for the Privacy Act system of records as outlined in the notices. The request will be processed by VHA within 20 work days.

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

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

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.

1)The individual who initiated a record or request in LEAF and later discovered error or omission can go back to the record and correct it. 2) When information is collected by LEAF administrator and the error or omission is discovered later, the individual can ask an administrator to correct it.

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.

Users that enter the data have the same authority and ability to correct inaccurate or erroneous information. The only other person that can do this is the administrator, and that is only at the user's request. LEAF users can find their respective LEAF administrators by viewing all people included on the cc line of their "LEAF Welcome" email. All changes and corrections are noted in the database logic and can be traced and tracked if needed.
VHA has a documented process for individuals to request inaccurate PII be corrected or amended and a process for review to determine if correction or amendment is appropriate. The policy complies with both the Privacy Act, VA regulations and the HIPAA Privacy Rule and is described in detail in VA Directive 1605.01 Privacy and Release of Information. Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SORN. Every VHA Privacy Act SORN contact information on Contesting Record Procedure which informs the individual who to contact for redress. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.

LEAF allows users to directly access and update their information before workflow processes are considered resolved/closed out.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:

<u>Privacy Risk:</u> There is a risk that an employee may not know how to obtain access to their records or how to request corrections to their records.

<u>Mitigation:</u> VA staffs Release of Information (ROI) offices at facilities to assist employees with obtaining access to their own records containing personal information.
Individuals are encouraged to use the redress procedures discussed above to request edits to their personal records retained about them, and are notified through the LEAF interface that they may access and update their information.

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 must first have a VA Network account assigned by the VA Office of Information Technology to initially log into the system.

Once logged in, site administrators establish access to data by assigning group based access to their business process workflow.

The criteria for access to PII data is established by the Site Administrator, Supervisor, and Privacy Officer.

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?

N/A, LEAF data is only available within its implanting agency. For example, LEAF within VA may only be accessed by people with a VA network account.

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.

Roles are defined by site administrators. For example, on https://leaf.va.gov, 1) All users have read-only access to the main page, 2) The “LEAF Coach” role has access to amend and act upon requests, 3) The “Site Administrator” role has access to modify the “LEAF Coach” role.

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.

VA Contractors that are an active member of the GAL and that have gone through the VA onboarding security process will have access to the system and are operating under VA Policy and security practices. VA Contractors that do not meet both of the above-mentioned clearances and a need to know, will not have access to the system.
Those Contractors that do have access to the system to design and maintain, are operating under a contract and MOU on distinct functions they are required and authorized to perform. These contracts and MOUs are reviewed and re-approved or disapproved on an annual basis. These contracts have established Quality Assurance Plans and actions to be taken if there is a breach in contract.

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.

All users are required to complete initial and annual Security Awareness, PII, and HIPAA training (If PHI is present), and sign the National Rules of Behavior as provided via the TMS system and enforced for all VA account holders. Maintaining a current VA network login account is a prerequisite to LEAF access.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 10/26/2022
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 2/17/2022
5. *The Authorization Termination Date:* 2/17/2025
6. *The Risk Review Completion Date:* 1/5/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A, Completed

Section 9 – Technology Usage

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

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

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

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)*

Yes; LEAF is hosted in VA Enterprise Cloud - AWS GovCloud (US) HIGH, which is FEDRAMP authorized. Infrastructure as a Service (IaaS)

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.*

LEAF is hosted in the VA Enterprise Cloud (VAEC) AWS

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.

VAEC has established a series of contract vehicles to support the acquisition of cloud and the operation of the VAEC. The VAEC is the hosting environment for all OI&T cloud applications, in order to ensure consistent utilization and execution in alignment with the VA Cloud Strategy. The enterprise cloud solutions office (ECSO), under the technical auspices of the Executive Director for Demand Management, is the governing authority for utilization of all VA cloud assets. All organizations, contracting teams, and program/project managers are expected to cooperate with the ECSO to ensure an orderly transition of governance of the current cloud-related aspects of their contracts to the ECSO. The ECSO will collect only those personal data elements required to fulfill an official function or mission. Those collections will be conducted by lawful and fair means.

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

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

The VAEC is a multi-vendor platform for the development and deployment of VA cloud applications. The VAEC also provides a set of common services such as authentication and performance monitoring, accelerating, and simplifying the development of new applications in or migration of existing applications to the cloud. In accordance with the Cloud Policy Memorandum dated October 29, 2019, LEAF project managers and business owners will ensure that all efforts comply with IT security, privacy, and networking requirements.

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).

Software scripts are used for a variety of functions, including installing LEAF sites, generating reports, scheduling emails, or performing data backups. Automations involving data backups can potentially copy PII/PHI information into secure backup environments within the VA Enterprise Cloud.

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

ID	Privacy Controls
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.

Lynn A Olkowski Digitally signed by Lynn A Olkowski
Date: 2023.09.08 11:35:03 -05'00'

Privacy Officer, Lynn A Olkowski

RUSTINE JOHNSON Digitally signed by RUSTINE JOHNSON
Date: 2023.09.06 08:18:20 -05'00'

Information System Security Officer, Rustine Johnson

MICHAEL GAO Digitally signed by MICHAEL GAO
Date: 2023.09.08 12:41:02 -04'00'

Information System Owner, Michael Gao

APPENDIX A-6.1

The following text is a Privacy Act notice for a business process implemented within LEAF. Individually implemented processes may differ in specific language or presentation.

> **Authority:** Pursuant to 38 U.S.C. §§ 7301(b), 7318(b), 7421, Executive Order 13991 and OPM approved variation to the requirements of 5 CFR 339.205, approval letter dated August 11, 2021 and VHA Directive 1193.01, we are authorized to collect this information. The authority for the system of records notices (SORN) associated with this collection of information, OPM/GOVT-10, Employee Medical File System of Records, 75 Fed. Reg. 35099 (June 21, 2010), amended 80 Fed. Reg. 74815 (Nov. 30, 2015), for title 5 employees, and 08VA05, Employee Medical File System Records (Title 38)-VA, for title 38 employees, also includes 5 U.S.C. chapters 33 and 63 and Executive Order 12196, Occupational Safety and Health Program for Federal Employees (Feb. 26, 1980). Providing this information is mandatory, and we are authorized to impose penalties for failure to provide the information pursuant to applicable Federal personnel laws and regulations.
>
> **Purpose:** This information is being collected and maintained to promote the safety of Veterans and patients receiving care and interacting with Health Care Personnel in VA health care facilities, as well as colleagues interacting with health care staff who work to service Veterans as part of the health care systems, consistent with guidance from Centers for Disease Control and Prevention and the Occupational Safety and Health Administration.
>
> **Routine Uses:** While the information requested is intended to be used primarily for internal purposes, in certain circumstances it may be necessary to disclose this information externally, for example to disclose information to: a Federal, State, or local agency to the extent necessary to comply with laws governing reporting of communicable disease or other laws concerning health and safety in the work environment; to adjudicative bodies (e.g., the Merit System Protection Board), arbitrators, and hearing examiners to the extent necessary to carry out their authorized duties regarding Federal employment; to contractors, grantees, or volunteers as necessary to perform their duties for the Federal Government; to other agencies, courts, and persons as necessary and relevant in the course of litigation, and as necessary and in accordance with requirements for law enforcement; or to a person authorized to act on your behalf. A complete list of the routine uses can be found in the SORNs associated with this collection of information.
>
> **Consequence of Failure to Provide Information:** Providing this information is mandatory. Unless granted a legally required exception, all Health Care

Personnel are required to be vaccinated against COVID-19 and to provide documentation concerning their vaccination status to their employing agency. Unless you have been granted a legally required exception, failure to provide this information may subject you to disciplinary action, including and up to removal from Federal service.

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