Privacy Impact Assessment for the VA IT System called:

VA Light Electronic Action Framework (LEAF) Cloud Assessing

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

Date PIA submitted for review:

October 05, 2021

System Contacts:

<table>
<thead>
<tr>
<th>System Contact</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Rita Grewal</td>
<td><a href="mailto:Rita.Grewal@va.gov">Rita.Grewal@va.gov</a></td>
<td>202-632-7861</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Rustine Johnson</td>
<td><a href="mailto:Rustine.Johnson@va.gov">Rustine.Johnson@va.gov</a></td>
<td>414-584-2000 x42194</td>
</tr>
</tbody>
</table>
### 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 business process management tool, a Software-as-a-Service, that empowers its users to rapidly digitize existing processes, and to create standardized digital workflows, forms, and custom reports.

LEAF’s mission is to empower VA employees and business lines with rapid development capabilities that are scalable and cost-effective to help deliver world-class service to Veterans.

### 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:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- 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.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes
- Whether the completion of this PIA could potentially result in technology changes
• 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 Light Electronic Action Framework (LEAF) falls under the purview of The Office of Information of Technology (OIT), Franchise Budget Office. LEAF is a business process management Software-as-a-Service that empowers its users to rapidly digitize existing processes, and to create standardized digital workflows, forms, and custom reports. LEAF’s mission is to empower VA employees and business lines with rapid development capabilities that are scalable and cost-effective to help deliver world-class service to Veterans.

LEAF stores all VA employee emails, and all forms of PII/PHI as outlined in the table on the next page. Information is pulled from the VA Global Address List (GAL) or input directly into LEAF by VA Employees or Contractors with an active OIT network account. As of February 2021, LEAF has an active monthly user base of more than 105,000 internal VA employees and processes over 180,000 VA requests monthly. Typical clients include any VA employee or contractor who initiates and/or approves a request for their respective business process.

LEAF is a nationally available web service hosted within the VA Enterprise Cloud. LEAF is a workflow engine and contains the information pertaining to workflow initiation or approval: administrative and clinical support processes and workflows. Since the LEAF system can be used to automate any administrative or clinical workflow within a Veterans Affairs Medical Center (VAMC), the types of data processed would include all data types common to a VAMC. As LEAF is process agnostic, sites may use LEAF for OIG investigative oversight and many portals utilize LEAF for resource expenditures and tracking.

LEAF does not directly share information with any other VA systems. Information may be accessed by individuals who have a valid VA network account and who also have access to the respective database.

PII security controls are maintained consistently as all sites use approved encryption technologies provided through the VA Enterprise Cloud for data at rest and data in transit.

On March 18, 2021, VA LEAF (Cloud) Assessing received a one-year ATO. Its VA System Inventory (VASI) number is 2195, and is covered under the following SORNs:


General Personnel Records (Title 38)-VA: July 20, 2000, 65 FR45131

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:
It is not anticipated that this PIA will result in any changes to business processes. LEAF development team continually assesses security posture and changing business requirements and adds features accordingly. However, it is not anticipated that this PIA will result in any changes to technology. Revision and approval of SORN will not be required.

The system uses cloud technology and is FedRAMPed. LEAF has a contract with VA Enterprise Cloud (AWS), encompassing the principal “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” (NIST 800-144). If privacy related data is disclosed, intentionally or unintentionally, moderate harm could occur.

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.

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 Account Information
- Health Insurance Beneficiary Numbers
- Account numbers
OIG Investigation Findings

***PII Mapping of Components***

LEAF consists of 2 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by LEAF and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**

*Note:* Due to the PIA being a public facing document, please do not include the server names in the table.

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web-based application</td>
<td>Yes</td>
<td>No</td>
<td>See section 1.1 for complete list</td>
<td>Required for business processes. As LEAF is process agnostic, examples have been given in the system overview</td>
<td>Encryption in transit, Session Timeout, Masked Fields, Two-factor authentication</td>
</tr>
<tr>
<td>Database</td>
<td>Yes</td>
<td>Yes</td>
<td>See section 1.1 for complete list</td>
<td>Required for business processes. As LEAF is process agnostic, examples have been given in</td>
<td>Encryption in transit, Encryption at rest, Virtual Private Network,</td>
</tr>
</tbody>
</table>
1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The Health Profession Trainees provide the information to a VA user who serves as the administrator with access to LEAF to facilitate the entry to the system. Source of the information in LEAF is the end-users who produce or consume the digital forms and processes stored in LEAF. LEAF does not require information from sources other than the individual. LEAF’ end users include both VA employees who digitize forms and VA employees who complete those same forms. Form types vary and can range from human resources to clinic cancellation requests.

LEAF collects the following information from the GAL: employee name and contact information. This information is used to facilitate usability: an employee name and office is more understandable than a convoluted account name.

LEAF imports data from the VA Central Data Warehouse (CDW).

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?
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.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information in LEAF is collected by direct input into digital form by end-user. LEAF also
creates reports based on parameters given by end-users. LEAF’s end users include both VA
employees who digitize forms and VA employees who complete those same forms.

1.4 How will the information be checked for accuracy? How often will it be checked?

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.

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.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and
Integrity Board.

Information collected within LEAF is reviewed by approving officials designated by the
individual administrator of a LEAF portal. The lifecycle of the information is typically very
short, as it is not relevant after a workflow has been completed. Information is then only archived
for the duration of the individual portal’s records retention policy.

Data relating to individuals with a VA network account is obtained from the GAL automatically
through a direct data connection. Individuals therefore follow standard processes, such as
submitting an OIT helpdesk ticket to update their information in GAL.

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.
On March 18, 2021, LEAF-S (Cloud) received a one-year ATO. Title 38 USC 501 (a) and Section 7304(a)(2) and Executive Order 9397.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information
Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

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

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

**Privacy Risk:** Veterans Health Administration utilizes LEAF for both the Presidential Transition Team, Action Tracking and the Veterans Health Administration Reorganization. All use cases are strategic, sensitive, and outline long-term goals and actions for the agency and would place the Federal strategic plans in a position of sensitive vulnerability and capability. C=M; I=M; A=L. LEAF can be used as the Disaster Response Hub to facilitate Health Care Providers volunteering their time to search National Disaster areas. The LEAF database will then be housing Provider information, dates and times of response to the National Disaster, credentialing information (future use), background information that supports development of federal continuity of operations plans can reveal sensitive vulnerabilities, capabilities. C=M; I=M; A=M. The data housed in LEAF are OIG Reports with action status and determination. Data includes; Patient Names, Patient SSN, Patient Diagnosis, Physician Name and Title, Actions Taken by the Physician, Negative Outcomes, which generated an OIG Finding, Actions toward Resolution of the Negative Outcome. C=H; I=H; A=M. Staff recruitment, selection, training, separation, Union grievances, succession planning; and all the personal information, which is required to perform all these human capital management actions information can be housed in LEAF. With the current climate between some Veterans with their trust with the Veterans Health Administration, this could place these Providers in a position as potential targets for retaliation by criminal
elements. C=M; I=L; A=L. Information regarding staff recruitment and selection of critical need, specialized providers and the bonuses they receive, and or SES level staff with pay for performance where the public may not support the decisions can be housed in LEAF. With the current climate between some Veterans with their trust with the Veterans Health Administration, this could place these Providers in a position as potential targets for retaliation by criminal elements. C=M; I=L; A=L. The LEAF System contains sensitive personal information – including social security numbers, names, and protected health information – on VA employees. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may occur.

**Mitigation:** VA has policies and procedures to protect this business practice and LEAF has a need-to-know security function to limit visibility into individual requests of this type. These actions are absolutely relevant and necessary to accomplish the specific mission of the VA. Veterans Health Administration (VHA), facilities deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors within the region. Security measures include access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance. Furthermore, LEAF implements 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.*

LEAF helps modernize business processes by reducing manual, labor-intensive steps in workflows. For example, at the Portland, Oregon VA Medical Center (VAMC), LEAF is being utilized to provide real-time graphical dashboard of quality-of-care indicators to improve care delivery. At VA headquarters in Washington D.C., LEAF is expediting telehealth care delivery when disasters strike with a portal where healthcare providers can volunteer their services online. At Phoenix VAMC, LEAF is used to help identify and quickly fill unexpected staffing absences to cover scheduled appointments. At the writing of this document, there were over 85 different use cases in practice. All use cases are to conduct business within the VA Enterprise and provide services to our Veterans.
2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

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

2.3 How is the information in the system secured?

2.3a What measures are in place 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. This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?
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.

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.

OIT maintains security procedures when granting GAL access and PIV badges, as this access is a prerequisite for using LEAF.

---

**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 Number(s),  
Personal Email Address,  
Emergency Contact Information (Name, Phone Number, etc. of a different individual),  
Financial Account Information,  
Certificate/License numbers,  
Vehicle License Plate Number,  
Internet Protocol (IP) Address Numbers,  
Current Medications,  
Previous Medical Records,  
Medical Record Number,  
OIG Investigation Findings

All information listed above is manually input by end users (all of whom are VA employees).

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

At the time of this writing, all data entered into LEAF will be maintained until the individual that generated it chooses to delete it, or the administrator of the site chooses to delete it. This is not in compliance with the NARA retention schedule. The LEAF Team is currently setting up a framework to help site administrators be in compliance with the NARA schedule.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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.
3.4 What are the procedures for the elimination of SPI?

*Explain how records are destroyed or eliminated at the end of the 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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?  
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research*

LEAF data is not used for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

*Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.*
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.

**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 3.10 (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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Information and Technology, VA Central Data Warehouse</td>
<td>Promote the health and safety of the Federal workforce and the efficiency of the civil service</td>
<td>Name, Social Security Number, Date of Birth, Mother’s Maiden Name, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information (Name, Phone Number, etc. of a different individual), Financial Account Information, Certificate/License numbers, Vehicle License Plate Number, Internet Protocol (IP) Address Numbers, Current Medications,</td>
<td>Secure database connection using Microsoft SQL Server protocols</td>
</tr>
</tbody>
</table>
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 shared/received with the Program Office or IT system | Describe the method of transmittal

| Previous Medical Records, Medical Record Number, OIG Investigation Findings, metadata including timestamps |

---

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

Follow the format below:

**Privacy Risk:** Information may be accessed by 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 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.
Roles are defined by site administrators. For example, 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.

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 3.11 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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
</table>
If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

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

**Mitigation:** 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 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?
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. If notice was provided in the Federal Register, provide the citation.

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

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. This question is 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.

Federal Register /Vol. 73, No. 229
Administrative Data Repository – VA
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: Published Prior to 1995, 08VA05


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

Upon employment, employees have information collected about them. If they decline to give information they may or may not get hired depending on what information that is being withheld.

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

VHA 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 VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by VHA 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.

VHA 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 do so unless there is a statute or regulation that requests the collecting and then consent is not necessary but when legally required VHA 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 Privacy Practices VHA HK 1605.04 here
https://www.va.gov/vhapublications/publications.cfm?pub=2

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.

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 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?

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.

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).

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. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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.
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 administrator to correct it. It is done by contacting leaf@va.gov

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.

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.

7.3 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 LEAF Program Office provides training on a monthly basis and has a User’s Guide with instructions on how to perform this function.
Employees are informed of the amendment process by many resources to include the Notice of Privacy Practice (NOPP) which states:

**Right to Request Amendment of Health Information.**

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a “Statement of Disagreement”
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Information can also be obtained by contacting the facility ROI office.

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.

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

*Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.*

Individuals are encouraged to use the formal redress procedures discussed above to request edits to their personal records retained about them.

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.
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 an employee may not know how to obtain access to their records or how to request corrections to their records

**Mitigation:** VHA 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 formal redress procedures discussed above to request edits to their personal records retained about them.

**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?**

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

*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?*

*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.*

*This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.*

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.

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 thru the PIV 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, 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 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?

If Yes, provide:

1. The Security Plan Status,
2. The Security Plan Status Date,
3. The Authorization Status,
4. The Authorization Date,
5. The Authorization Termination Date,
6. The Risk Review Completion Date
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

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

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

The Security Plan status is current, and the date is February 2, 2021. Per the approval of the Deputy Assistant Secretary, Enterprise Program Management Office (EPMO) [the VA Authorizing Official (AO)], On March 18, 2021, LEAF-S (Cloud) received a one-year ATO. The risk review (risk assessment report) was completed on August 24, 2021. The FIPS 199 classification is HIGH.

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, 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.
This question is related to privacy control UL-1, Information Sharing with Third Parties.

Yes; LEAF is hosted in AWS GOVCloud HIGH, which is FEDRAMP authorized.

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Infrastructure as a Service (IaaS)

9.3 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)

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.

The VAEC (VASI ID 2438) will maintain and operate in accordance with the application and VAEC service level agreements (SLAs), and LEAF will operate in its current environment in parallel as applicable. When the VA collects personal data from an individual, the VA will inform him or her of the intended uses of the data, the disclosures that will be made, the authorities for the data’s collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act System of Records Notice has been published in the Federal Register and posted on the VA Systems of Records website. As such the VA will retain ownership rights over the data only for as long as necessary to fulfill the purposes for which it is collected. These records will be destroyed in accordance with established NARA records schedule.
9.4 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.

9.5 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, speeding 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.
9.6 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 9. References

### Summary of Privacy Controls by Family

<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>Authority and Purpose</td>
</tr>
<tr>
<td>AP-1</td>
<td>Authority to Collect</td>
</tr>
<tr>
<td>AP-2</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>AR</td>
<td>Accountability, Audit, and Risk Management</td>
</tr>
<tr>
<td>AR-1</td>
<td>Governance and Privacy Program</td>
</tr>
<tr>
<td>AR-2</td>
<td>Privacy Impact and Risk Assessment</td>
</tr>
<tr>
<td>AR-3</td>
<td>Privacy Requirements for Contractors and Service Providers</td>
</tr>
<tr>
<td>AR-4</td>
<td>Privacy Monitoring and Auditing</td>
</tr>
<tr>
<td>AR-5</td>
<td>Privacy Awareness and Training</td>
</tr>
<tr>
<td>AR-7</td>
<td>Privacy-Enhanced System Design and Development</td>
</tr>
<tr>
<td>AR-8</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>DI</td>
<td>Data Quality and Integrity</td>
</tr>
<tr>
<td>DI-1</td>
<td>Data Quality</td>
</tr>
<tr>
<td>DI-2</td>
<td>Data Integrity and Data Integrity Board</td>
</tr>
<tr>
<td>DM</td>
<td>Data Minimization and Retention</td>
</tr>
<tr>
<td>DM-1</td>
<td>Minimization of Personally Identifiable Information</td>
</tr>
<tr>
<td>DM-2</td>
<td>Data Retention and Disposal</td>
</tr>
<tr>
<td>DM-3</td>
<td>Minimization of PII Used in Testing, Training, and Research</td>
</tr>
<tr>
<td>IP</td>
<td>Individual Participation and Redress</td>
</tr>
<tr>
<td>IP-1</td>
<td>Consent</td>
</tr>
<tr>
<td>IP-2</td>
<td>Individual Access</td>
</tr>
<tr>
<td>IP-3</td>
<td>Redress</td>
</tr>
<tr>
<td>IP-4</td>
<td>Complaint Management</td>
</tr>
<tr>
<td>SE</td>
<td>Security</td>
</tr>
<tr>
<td>SE-1</td>
<td>Inventory of Personally Identifiable Information</td>
</tr>
<tr>
<td>SE-2</td>
<td>Privacy Incident Response</td>
</tr>
<tr>
<td>TR</td>
<td>Transparency</td>
</tr>
<tr>
<td>TR-1</td>
<td>Privacy Notice</td>
</tr>
<tr>
<td>TR-2</td>
<td>System of Records Notices and Privacy Act Statements</td>
</tr>
<tr>
<td>TR-3</td>
<td>Dissemination of Privacy Program Information</td>
</tr>
<tr>
<td>UL</td>
<td>Use Limitation</td>
</tr>
<tr>
<td>ID</td>
<td>Privacy Controls</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

RITA K GREWAL
114938
Digitally signed by RITA K GREWAL 114938
Date: 2021.10.19 21:01:25 -04'00'

Privacy Officer, Rita Grewal

rustine p.
johnson 255238
Digitally signed by rustine p. johnson 255238
Date: 2021.10.20 08:28:13 -05'00'

Information Systems Security Officer, Rustine Johnson

Michael L. Gao
106871
Digitally signed by Michael L. Gao 106871
Date: 2021.10.20 09:43:06 -04'00'

System Owner, Michael Gao
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).

Federal Register /Vol. 73, No. 229

Administrative Data Repository – VA


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: Published Prior to 1995, 08VA05