Privacy Impact Assessment for the VA IT System called:

Managed Services – FOIAXpress™ Assessing

CRR VACO FOIA Support Office

VACO

eMASS ID 193

PIA submitted for review:

03/04/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.facemire@va.gov OITPrivacy@va.gov	202-632-8423
Information System Security Officer (ISSO)	Neil Cruz	Neil.Cruz@va.gov	202-632-7422
Information System Owner	Ramon L. Morales	Ramon.morales@va.gov	512-550-4178

Abstract

The abstract provides the simplest explanation for "what does the system do for VA?".

FOIAXpress™ is designed specifically to automate Freedom of Information Act (FOIA) and Privacy Act (PA) requests.

Overview

The overview is the most important section of the Privacy Impact Assessment (PIA). A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

The Department of Veterans Administration Managed Service - FOIAXpress™ Assessing (FOIAXpress™) is a VA Managed Service web-based SaaS application that automates the FOIA business process for all FOIA requests received at the various VA departmental FOIA offices. FOIAXpress™ is designed specifically to automate Freedom of Information Act (FOIA), and Privacy Act (PA) request case processing, including request tracking and management, document management, electronic redaction, fee management and invoicing, and annual reporting. FOIAXpress™ provides compliance with FOIA/PA regulations with a powerful application that will provide VA with a tool that will transform their FOIA/PA experience from a cumbersome, manual process to an automated, electronic one. The FX system processes FOIA request data received by FOIA users. FOIA data consists of requests for information received from the public which includes personal identification information and financial information related to the processing of FOIA request. Nevertheless, the confidentiality of system data must be safeguarded against disclosure The FOIAXpress™ is web-based application using Microsoft IIS server and .NET technology. The database is SQL server. Users access the application through browser using HTTPS protocol Each customer has their own instance of virtual servers. Only agency network is whitelisted to access the agency instance of FOIAXpress™. For example, VA instance is accessible only from VA network. Users must be in the VA network to access the network using Active Directory SSO in compliance with MFA requirements. The FOIAXpress™ application server (Microsoft IIS server) is connected to FOIAXpress™ database server. Only user metadata is stored in FOIAXpress™ database.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

VA Controlled / non-VA Owned and Operated

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

Approximately 200,000 Individuals information would be present. The information is any VA record that would be collected and subject to the FOIA by the Department of Veterans Affairs.

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

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

The law provides individuals with a statutory right of access to certain federal agency records. FOIAXpress™ is the official VA mandatory FOIA tracking system.

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

FOIAXpress™ is mapped to the Public Access Link (PAL) and the Electronic Document Review (EDR) components. Video and Audio redactions take place in the external Veritone Application that shares information with FOIAXpress™.

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

Yes

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

FOIAXpress™ application operates within the FedRAMP approved AINS/OPEXUS eCase network.

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

H. What is the citation of the legal authority?

- FOIA Improvement Act of 2016
- 5 U. S. C. 552, Freedom of Information Act, 1967
- 5 U. S. C. 552a, Privacy Act, 1974
- 18 U. S. C. 1030 (a) (3), Fraud and related activity in connection with computers
- CFR 38 Part 1& 2
- 5 U.S.C. 301
- 38 U.S.C. 501
- FOIA Improvement Act of 2016, Public Law 114–185

I. What is the SORN?

119VA005R1C - Freedom of Information Act (FOIA) Records - VA

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

No

4. System Changes

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

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

I. Will the technology changes impact information collection and sharing?

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

Section 1. Characterization of the Information

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

1.1 Information collected, used, disseminated, created, or maintained in the system.

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

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

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

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

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

Other PII/PHI data elements: Biometrics, driver's license number and driver's license photo

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

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

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

Information contained within FOIAXpress™ is provided directly by the requesting individual or their representative or from PAL. Individuals who appeal VA denial of their FOIA requests, individuals who requests, appeals, and/or records have been referred to VA by other agencies, and, in some instances, attorneys or other persons representing individuals submitting such requires and appeals, individuals who are the subjects of such requests, other government litigators and/or VA personnel assigned to handle such requests or appeals.

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 inherent nature of FOIA is to provide reasonable access to all Government information to the public. This ensures that the sources of the information are not limited in scope, source, or volume due to the federal laws and precedent surrounding the subject. The VA adamantly monitors the information released in accordance with requests or preemptive releases that benefit the public.

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

FOIAXpress™ provides rudimentary dashboard capabilities that performs superficial analysis of database numbers (e.g., date stamps, status, users, etc.). Reporting capabilities are available through FOIAXpress™ but are only reflections of database information listed previously.

1.3 Methods of information collection
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

Requests: Individuals request information either electronically or in written form. There is no specific form used by requesters. Information is collected when an individual provides a written FOIA request in any form or format. The request is scanned into the system and used to determine the next step in the process. The requests are not collected by VA but are maintained as the method of contacting the individual or organization to reply to his/her request.

Response: Responses are in accordance with guidance from the Office of Management and Budget (OMB), contained in M-04-04 E-Authentication Guidance for Federal Agencies, which requires agencies to review new and existing electronic transactions to ensure that authentication processes being used provide the appropriate level of assurance. VA system owners are responsible for compliance with this process.

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

There are no specific forms to be used for requests by individuals. VBA forms available for FOIA use include: VA Form 20-10206, Freedom of Information Act (FOIA) or Privacy Act (PA) Request, VA Form 20-10207, Priority Processing Request, and VA Form 20-10208, Document/Evidence Submissions.

1.4 Information checks for accuracy, and how often will it be checked.

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

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

The data stored in FOIAXpress™ is checked for accuracy on a quarterly and annual basis prior to running the required quarterly and annual reports for submission to the Department of Justice. A thorough review of the numbers and request data is done prior to pulling the reports. Reports can be generated in the application to validate the data imported to the system. Application does not check validity when receiving it from users.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

VA employees and contractors processing FOIA requests will enter data into the system and verify the data after entry. Data is verified against the FOIA requests received from FOIA requesters. FOIAXpress™ provides an 'audit report', which details 'what event occurred' (e.g., the action taken), 'when' (e.g., date/time), where the event occurred (e.g., specific feature/function), the source of the event (e.g., user's email), and identify (e.g., username).

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in

addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The following are laws, regulations, and policies that affect the system:

- FOIA Improvement Act of 2016
- 5 U. S. C. 552, Freedom of Information Act, 1967
- 5 U. S. C. 552a, Privacy Act, 1974
- 18 U. S. C. 1030 (a) (3), Fraud and related activity in connection with computers
- CFR 38 Part 1& 2
- SORN 119VA005R1C - Freedom of Information Act (FOIA) Records – VA
- 5 U.S.C. 301
- 38 U.S.C. 501
- FOIA Improvement Act of 2016, Public Law 114–185

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: The amount of data collected consist of FOIA records of inquiries, replies, and related correspondence; in the case of FOIA, Privacy Act, and mandatory declassification files, appeals and other records; administrative background files for formal information releases, and records relating to inappropriate release of privileged information.

Mitigation: The exposure is mitigated by safeguarding records in FOIAXpress™ in accordance with applicable rules and policies, including all applicable VA automated systems security and

access policies. Strict controls have been imposed to minimize the risk of compromising the information that is stored. Access to the computer system containing the records in this system is limited to those individuals who have been granted system access rights, and those who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	Internal Use	External Use
Name Full Sociate Security Number Date of Birth Mother's Maiden Name Personal Mailing Address Personal Phone Number(2) 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 Internal Protocol (IP) Address Numbers Medications Medical Records Race/Ethnicity Tax Identification number Medical Record Number Sex Integrated Control Number (ICN) Military History/Service Connection	FOIAXpress™ Service	Not used

Next of Kin Business Email Address Biometrics Driver's License number Driver's License Photo		
Name Address Phone Number Email Address	Public Access Link (PAL)	Public Access Link (PAL)
Name Personal Address Personal Phone Number Personal Email Address Business Address Business Phone Number Business Email Address Financial Information	Pay.gov	Pay.gov
Electronic Document Review (EDR)	N/A	N/A
Biometrics		Veritone
Name Mailing Address Phone Number Financial Information		Pay.gov

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

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

The system does not analyze the data inside the record. The system's primary function is to track FOIA cases and provide analytical data on the number of open cases, late cases, number of appeals and other statistical data. FOIAXpress™ management obtains reports on the number of FOIA requests currently over twenty days old, the number of requests waiting to be processed, the number and type of exemptions used, number of appeals filed, number of backlogged requests, the categories of records being requested, and the category of requests.

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.

Any newly derived information will be placed in the individuals existing record.

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

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

TLS 1.2 is used to encrypt the data in transit and Microsoft 256-bit AES encryption is used for data at rest.

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

The data (SSN number) will not be displayed when user inputting the SSN. It will be masked and will not display when user entering the SSN number.

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

Providing annual security trainings to the users, developers.
Updating policies and procedures documents every year.
Providing access control (user level permissions) in the application.
FISMA and FedRAMP compliance.

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

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

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

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

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

2.4a How is access to the PII determined?

Users requiring access to FOIAXpress™ will contact the VACO FOIA office. The user will then accomplish training and provide the certification to the VACO FOIA office who will approve the access to FOIAXpress™. The FX Admin will create an account and will provide the user an encrypted password for access.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

A detailed email listing the required for completion of required training is sent to each individual requesting an account in FOIAXpress™. Once the individual has completed the required training, their account is created.

2.4c Does access require manager approval?

Yes

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

Yes

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

The FOIA officer at each facility/site is responsible to control access of users to prevent any PII information leakage. AINS/OPEXUS system administrators are responsible for protecting PII information on the database by encrypting the information.

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*

Requester details:

- Requester name (First Name*, Last Name*)
- Shipping address (Street, City, State, Zip, Country*)
- Other address (Street, City, State, Zip, Country)-if different from shipping address

- Billing address (Street, City, State, Zip, Country)-if different from shipping address
- Request description (e.g., what the requester is asking for in their FOIA/PA request)
- If fees/invoices and payment apply to a request, then the system may track the amount due.
- Requester name (First Name*, Last Name*)
- Shipping address (Street, City, State, Zip, Country*)
- Other address (Street, City, State, Zip, Country)-if different from shipping address
- Billing address (Street, City, State, Zip, Country)-if different from shipping address
- Request description (e.g., what the requester is asking for in their FOIA/PA request)
- If fees/invoices and payment apply to a request, then the system may track the amount due.

Additionally, FOIAXpress™ stores 'files' within the correspondence log for a request AND within the document management module (for responsive records), which may include but are not limited to the following:

- Correspondence from the requester (which may contain their name, address, phone number, etc.)
- Incoming request letter
- Clarification letter
- Fee agreement letter
- Correspondence to the requester (which may contain their name, address, phone number, etc.)
- Acknowledgement letter
- Final response letter
- Redacted responsive records
- Document management files
- Original (un-redacted) responsive records
- Redacted responsive records

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.

Retention period of FOIA requests and responsive documents are 6 years. The retention period of FOIA records in litigation are retained for ten years after the end of the fiscal year in which judgment was made or when all appeals have been exhausted, whichever is later. If the FOIA record deals with significant policy-making issues, it is a permanent record. A permanent record is one that has been determined by the National Archives and Records Administration (NARA) to have sufficient value to warrant its preservation in the National Archives of the United States. Permanent records include all records accessioned by NARA into the National

Archives of the United States and later increments of the same records, and those for which the disposition is permanent on SF 115s, Request for Records Disposition Authority, approved by NARA on or after May 14, 1973. FOIA records are retained in accordance with National Archives and Records Administration's General Records Schedule 14. The General Records Schedule 14 covers certain records pertaining to informational services performed by Government agencies in their day-today affairs and in their relations with the public, including records created in administering Freedom of Information Act and Privacy Act (FOIA) programs. These records consist of inquiries, replies, and related correspondence; in the case of FOIA, Privacy Act, and mandatory declassification files, appeals and other records; administrative background files for formal information releases, and records relating to inappropriate release of privileged information.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. Please work with the system VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

FOIA records are under the following General Records Schedule:

Administrative Files (001)
Access and Disclosure and Appeal (020)
Records Tracking (030)
Access Records (040)
Congressional ((070)
Reporting Records (080)
Virtual Public Access Library Files (180)
Transmittal No. 22 April 2010
General Records Schedule 14, Information Services

National Archives and Records Administration

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

Records are destroyed in accordance with GRS 4.2, Information Access, and Protection Records.

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.

Records are destroyed in accordance with NARA GRS 14 which prescribes the time period for the FOIA and Privacy Act case files and appeals. Records are transferred to the Federal Records Center. To date FOIAXpress™ logs have been retained for historical reporting purposes. 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), http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=416&FType=2. 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.

No, FOIAXpress™ does not use PII for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

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

Follow the format below:

Privacy Risk: 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 policies and procedures. 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.

Access to the system is protected with PIV implementation.

Mitigation: Information is restricted with user access and information is deleted based on the retention policy.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a **Managed Service – FOIAXpress™ Assessing** consists of **3** key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **FOIAXpress™** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

FOIAXpress™	Yes	Yes	• Name • Mailing Address • Zip Code • Phone Number • Email Address • SSN • Date of Birth • Medical Records	In support of FOIA Request Processing	Data Encryption
Public Access Link (PAL)	Yes	Yes	• Name • Address • Phone Number • Email address	Only required information is an email address.	.IPSec and inherited CSP structure
Electronic Document Review (EDR)	No	No	None	N/A	N/A
Pay.gov	Yes	Yes	• Name • Personal Address • Personal Phone number • Personal Email Address • Business Address • Business Phone Number	VA - FOIA collection account	443 TCP/IP

			• Business Email Address • Financial Information		

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

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

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

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

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

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

Data Shared with Internal Organizations

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

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

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

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

Follow the format below:

Privacy Risk: There is a possibility of sharing the information, such as case information, internally between authorized users.

Mitigation: The information shared within the confine of the system boundaries. As such, any individual accessing the information must have appropriate system roles and privileges. System roles and privileges are controlled by the System Administrator. Sharing of information in the system is based on Departmental FOIA officers with the appropriate privileges.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Veritone	Audio/Video Redaction	Biometrics	MOU/Contract	443 TCP/IP
Pay.Gov	Payment	Name Mailing Address Phone Number Financial Information	MOU/Contract	443 TCP/IP

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

Follow the format below:

Privacy Risk: Risks inherent to sharing information outside of the Department are present. The Confidentiality, Integrity, and Availability of PII/PHI are a known risk for computing in the FOIA sector.

Mitigation: Moderate impact: FOIAXpress uses AES 256, contract monitoring, FedRAMP monitoring, Department monitoring and eMASS compliance for shared information outside VA. FedRAMP Moderate environment adheres to NIST requirements. A contract is in place for this requirement.

Section 6. Notice

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

6.1 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

Notice is provided at the VA FOIA Home Page. Information is collected only insofar as it allows correspondence to be sent to the requestor. Such information is not "collected" but is provided to VA to allow responses to the requester of the information. VA Public Access Link and SORN 119VA005R1C - Freedom of Information Act (FOIA) Records – VA.

6.1b If notice was not provided, explain why.

Notice included in Appendix A and states: You are about to access a U.S. information system; system usage may be monitored, recorded, and subject to Audit. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and the use of the system indicates consent to monitoring and recordings.

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

The notice for collection of information is documented and published in the Federal Register under Systems of Record Notice, 119VA005R1C for the Freedom of Information Act (FOIA) Records – VA.

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.

Requesters may decline to provide information (i.e., name and contact information) and remain anonymous, however, in order to process a FOIA request the FOIA Officer must have a return address, and or contact information to reply to a request. The result would mean their request may not be processed.

The Logon warning banner includes the following text:

**********WARNING**********
You are about to access a U.S. Government information system; system usage may be monitored, recorded, and subject to audit. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and use of the system indicates consent to monitoring and recording.
**********WARNING**********

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.

The only intended use is to respond to FOIA requests. Requester information is not provided outside of that scope.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must ensure that information is used only for the purpose articulated in the notice.
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.

Follow the format below:

Privacy Risk: Individuals may not be provided sufficient notice that their information is being collected.

Mitigation: If an individual is not given sufficient notice of their information being collected, the VA Privacy Office is notified and the PO will determine what actions to take (i.e., direct

additional training for the VA employee monitoring the individual whose PII was collected in accordance with SORN(s) requirements .

Section 7. Access, Redress, and Correction

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

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

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

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

The VACO FOIA Service created two mailboxes for the public the use to address any concerns or issues they may have. We have the FOIA Surveys mailbox and the VACO FOIA Help mailbox: vacofoiase@va.gov and foiahelp@va.gov. A FOIA requestor does not have access to the internal records beyond what is released to them through the PAL.

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)?

FOIAXpress™ is not exempt from access provisions under the privacy act.

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

FOIAXpress™ is a Privacy Act system.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The individual's information in FOIAXpress™ is only the information the individual provides. For reconciliation of any inaccurate or erroneous information in the record requires the individual to submit a request to the office that created and maintains those particular records.

FOIA officers at the affected site will update the individual's information based on the submitted request.

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 individuals are notified to submit a request to the office that created and maintains those particular records to correct any identified inaccurate or erroneous information. An acknowledgement letter is sent to the individual that provides the information and the steps to submit to the appropriate site/facility/area.

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.

An acknowledgement letter is sent to the requester that notifies the individual to the office that created and maintains the records in question.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: Individual is unable to obtain their record for required changes.

Mitigation: A request is submitted by the individual and an acknowledgement letter sent to them with instructions on obtaining their information and providing corrections.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

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

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

A detailed email listing of the required training to be complete is sent to FOIA approved individuals requesting an account in FOIAXpress™. Once the individual has completed the required training, their access is approved by the FX Admin Officer, and then the account is created.

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?

There are no users from other agencies with access to the VA FOIAXpress™ system.

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

Administrative: Access to configuration options, not SaaS administrators
Read/Write: Has ability to generate logged events and edit records
Read Only: No ability to generate logged events and cannot edit records

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

How frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have

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

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

Yes, contract individuals will process FOIA requests through FOIAXpress™ FX Admin. All necessary agreements are in place and held, reviewed, and initiated by the COR prior to granting access. Contractors will go through a Public Trust investigation and sign a NDA.

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

Yes, contract individuals have access to the system and PII.

8.2b. What involvement will contractors have with the design and maintenance of the system?

FOIAXpress™ is designed and maintained under contract with AINS/OPEXUS.

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 trained in accordance with VA Policy through the VA Talent Management System (TMS) on an annual basis, as well as additional formal and ad hoc trainings to include FOIAXpress™ basic level training. Contractors are trained in accordance with contractual requirements.

All VA staff and contractors with access to PII are required to complete VA Privacy and Information Security Awareness and Rules of Behavior Training (TMS Course # 10176). Completion of this training is required before granting access and must also be completed annually thereafter.

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

8.4a If completed, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* 4/9/2024
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* 7/17/2024
5. *The Authorization Termination Date:* 7/17/2025
6. *The Risk Review Completion Date:* 4/8/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

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

8.4b If not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

Cloud model: SaaS (AINS/OPEXUS eCase) an approved FedRAMP moderate system.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (* ***Refer to question 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

The VA retains IP rights and control over all VA Data. This is codified in the contract and PWS/SOW. Contract #: NNG15SD26B, §5.0 VA Information Custodial Language.

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.

CSP is responsible for ancillary data. All the data is stored in systems supporting FOIAXpress™ and are protected with access controls.

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 CSP is FedRAMP approved and is defined in the FOIAXpress™ contract.

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).

FOIAXpress™ does not use RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

TONYA FACEMIRE

Digitally signed by TONYA FACEMIRE
Date: 2025.05.12 13:42:20 -04'00'

Privacy Officer, Tonya Facemire

NEIL CRUZ

Digitally signed by NEIL CRUZ
Date: 2025.05.12 13:05:30 -04'00'

Information System Security Officer, Neil Cruz

RAMON MORALES

Digitally signed by RAMON MORALES
Date: 2025.05.12 12:51:58 -05'00'

Information System Owner, Ramon L. Morales

APPENDIX A-6.1

Notice is provided at the VA FOIA Home Page. Information is collected only insofar as it allows correspondence to be sent to the requestor. Such information is not "collected" but is provided to VA to allow responses to the requester of the information. VA Public Access Link and SORN 119VA005R1C - Freedom of Information Act (FOIA) Records – VA.

Authority: 5 U.S.C. § 552, 5 U.S.C. § 552a and 38 CFR § 1.550 through 1.562 Procedures for Disclosure of Records Under the Freedom of Information Act https://www.ecfr.gov/current/title-38/chapter-I/part-1/subject-group-ECFRc44d241fe38eae5. Specifically, 5 U.S.C. § 552 authorizes the collection of information, records, and related correspondence on individuals who have submitted requests for records to an agency. The Privacy Act, 5 U.S.C. § 552a(d), authorizes the collection of information, records, and related correspondence on individuals who have submitted requests under the provisions of the Privacy Act for records about themselves.

Purpose: The information collected by the Department of Veterans Affairs (VA) through the eFOIA Software as a Service, and the Public Access Link (PAL) is authorized by 5 U.S.C. § 552 and 5 U.S.C. § 552a.

Routine Use(s): The published routine uses to which the information is subject: VA will use this information to search for records responsive to your requests, track FOIA and Privacy Act requests, manage requester fees and payments where applicable, correspond with requesters, and provide responsive documents to requesters. VA uses the information collected by eFOIA and the PAL for authorized routine uses, including sharing with other federal government agencies and courts, as provided in the following System of Records Notices (SORNs) or their successors: Freedom of Information Act (FOIA) Records—VA (119VA005R1C)and SORN Other Government Agencies-VA (213VA045A1) and multiple Privacy Act-related SORNs found on the Department of VA's website at https://department.va.gov/privacy/system-of-records-notices/.

Disclosure: Disclosure of PII is voluntary. Individuals may refuse to provide their PII, thereby withdrawing their request. VA may not be able to respond to a request or locate responsive records if there is failure to describe the records sought in enough detail to allow VA personnel to locate them with a reasonable amount of effort. To the extent possible, the requester should include specific information about each record sought, such as the date, title or name, author, recipient, and subject matter of the document.

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)

Privacy, Policies, And Legal Information | Veterans Affairs.