Privacy Impact Assessment for the VA IT System called:

Electronic Permissions Access System (EPAS)

VA Central Office

Development, Security, and Operations

Date PIA submitted for review:

06/27/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Facemire, Tonya	Tonya.Facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	White, Crystal	Crystal.white@va.gov	813-340-3089
Information System Owner	Murray, Raleigh	Raleigh.murray@va.gov	214-274-1435

Abstract

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

Electronic Permission Access System (EPAS) is a web-based application designed to provide customized web forms presented filled out using any browser and workflows for a myriad of business functions involving request/approval processes such as but not limited to Elevated Privileges Request, VistA Access Request, and Employee Offboarding. Elevated Privileges requires Personally Identifiable Information (PII) to mail One Time Password (OTP) tokens to requestors homes. Veterans' Health Information Systems and Technology Architecture (VistA) systems currently require date of birth and social security numbers in the creation of VistA accounts.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Electronic Permission Access System (EPAS), VA Owned and VA Operated IS. The Program Office is Development, Security, and Operations.

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

EPAS is a web application designed to provide forms and workflows for a myriad of business functions involving request/approval system access. The primary of which is onboarding/offboarding staff within the VA.

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

Ownership/Control is from Raleigh Murray, FES Division Chief SharePoint & Web

2. Information Collection and Sharing

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

Greater than 10000

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

Electronic Permission Access System (EPAS) is a web application designed to provide workflows for a myriad of business functions involving request/approval system access. The system collects information from user Names, Addresses, SSN, DOB and Gender.The primary of which is electronically documenting the onboarding/offboarding of Veterans Health Administration (VHA) staff and documenting Elevated Privilege approvals within the Department of Veterans Affairs (VA). please provide response here

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

The EPAS system share no information outside the EPAS system itself.

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

The EPAS system is only operated from the Hines Data Center.

3. Legal Authority and SORN

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

A SORN is in development. The SORN for the system is currently in the process of being completed. The future SORN is Electronic Permissions Access System (EPAS)-VA (205VA005OPA31C)

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

Initial Sorn is in development,

D. System Changes

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

The completion of this PIA will not change any business processes.

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

This PIA should not result in any technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☐ Personal Phone Number(s)
☐ Personal Fax Number
☐ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers*
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender
☐ Integrated Control Number (ICN)

□ Military History/Service Connection

□ Next of Kin

□ Other Data Elements (list below)

PII Mapping of Components (Servers/Database)

Electronic Permission Access System (EPAS) consists of 6 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by EPAS and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
OITHINSQLEPAS.r02.med.va.gov	**Yes**	**Yes**	**Names, SSN, DOB, Address, Gender**	**VistA account creation**	**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

1.2 What are the sources of the information in the system?

The information is entered from individual users.

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

The information is collected from the individual as part of EPAS to receive approval for Elevated Privilege access.

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.

No information from outside sources required.

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

The system is not a source of information outside of EPAS.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

EPAS workflow information is collected directly from individuals or designed administrative staff. via the EPAS web application. No information is collected using other technology.

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

The information is not collected from a form.

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

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

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

EPAS information that is stored in the database is checked for accuracy by supervisors and respective administrative staff when the workflow is submitted. This workflow is a snapshot in time. Additional checks are completed quarterly during the ISSO quarterly reviews. EPAS does not validate the information on its system from an ancillary system. Workflows may be edited by appropriate staff with permission prior to final approval after manually checking against outside sources.

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

The EPAS system does not check for accuracy of the information entered or use a commercial aggregator.

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

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

EPAS collects the data and permissions needed for account managers to create VistA user accounts. EPAS becomes the documentation of the approval under Enterprise VistA, and all VHA facilities' VistA instances operate under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)

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

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

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

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: EPAS contains sensitive personal information – including social security numbers, names, gender, date of birth and home addresses. 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 result.

Mitigation: Viewing DOB or SSN is limited for viewing to those individuals with the proper authority and granted using access controls and training of employees and contractors. The EPAS portal utilizes Secure Socket Layer (SSL) to create an encrypted network path between client and server. The Database team encrypts the database using Transparent Data Encryption (TDE). The Hines Data Center provides physical security for the servers.

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.

EPAS digital Elevated Privileges and VistA Access Request documents are used by account managers to build a user's VistA account. Name, DOB, Gender and SSN are needed to create a user's account with proper identification in the VistA system. The employee's home address is used by Network Security group to issue a One Time Password (OTP) Token to network staff for Tier 3 network support.

2.2 What types of tools are used to analyze data and what type of data may be produced?

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

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

Microsoft SQL Server database tools are used by authorized OIT staff to generate reports used by the ISSO community for quarterly reviews. Database access follows the same encryption methods as EPAS and Microsoft Windows utilizing Active Directory security groups which restrict access to prevent unauthorized personnel access. No new or previously unutilized information about an individual is gathered. Once the EPAS request is completed it cannot be edited.

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.

Microsoft SQL Server database tools are used by authorized OIT staff to generate reports used by the ISSO community for quarterly reviews. Database access follows the same encryption methods as EPAS and Microsoft Windows utilizing Active Directory security groups which restrict access to prevent unauthorized personnel access. No new or previously unutilized information about an individual is gathered. Once the EPAS request is completed it cannot be edited.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

EPAS information is secured using Microsoft Active Directory security groups. Members with approved security group enrollment can access restricted data. Any PII data is only visible to staff with authorized permission to view such data using permission groups. The SQL Server database uses Transparent Data Encryption (TDE) to encrypt data at rest and SSL to encrypt data in transit.The EPAS portal also uses SSL to create an encrypted network path between client and server. The Database team encrypts the database using TDE.

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

No additional protections are employed specific to Social Security Numbers beyond security already in place for all PII.

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

All staff complete security training for Rules of Conduct to ensure PII is used appropriately and only for its intended purpose.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

EPAS contains user instructions on the landing page of the application which provide information for the use of the workflow. (https://epas.r02.med.va.gov/apps/myva/). To gain access to EPAS requires managers approval via access to assigned active directory groups. PII is recorded through weblogs on the web servers. OIT Field Enhancement Sustainment is responsible for ensuring safeguards are in place for PII.All VistA account managers are required to take Cyber Security and Ethics training.

EPAS users without approved permissions are unable to access PII. Only users with approved enrolled in Windows security groups can view data.

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

Criteria, procedures, controls and responsibilities are listed on the splash page/Help page.

2.4c Does access require manager approval?

Access to the application is via Active Directory logon permissions which requires manager approval.

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

PII is recorded through weblogs on the webservers.

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

OIT Field Enhancement Sustainment is responsible for ensuring safeguards are in place for PII.

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, Gender, Home Address, SSN and DOB are only collected when creating VistA and/or Active Directory user accounts.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted* *early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Office of Information & Technology (OI&T) Records: These records are created, maintained, and disposed of in accordance with Department of Veterans Affairs, Office of Information & Technology RCS 005-1. This allows OIT to maintain these records as long as the permission exist or until a replacement system is in place.

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

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

Office of Information & Technology (OI&T) Records: These records are created, maintained, and disposed of in accordance with Department of Veterans Affairs, Office of Information & Technology VA Record Control Schedule (RCS) 005-1.

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

Office of Information & Technology (OI&T) Records: These records are created, maintained, and disposed of in accordance with Department of Veterans Affairs, Office of Information & Technology VA Record Control Schedule (RCS) 005-1.

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.

EPAS is totally electronic, therefore no paper disposal is required. If records need to be eliminated from the database this can only be accomplished by those staff with specific permissions on the SQL database. Using the ServiceNow system a ticket is submitted to the Field Enhancement &

Sustainment group (IO.HBMC.FO.APP.FES.Web2). Only OIT staff members with access using Microsoft SQL Management Studio can remove records from the database.

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.

EPAS PII 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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information contained in the EPAS system 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 or breached

Mitigation: In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
N/A	No Information Shared		

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***

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

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

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

Follow the format below:

<u>Privacy Risk:</u> EPAS has a reporting database that provides limited information in the workflow of report without PII information. PII information is not shared internally. There is a risk that the data could be shared with an inappropriate VA organization or institution outside the system safeguards which would have a potentially catastrophic impact on privacy.

<u>Mitigation:</u> The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, 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.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A				

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

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

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

Follow the format below:

<u>Privacy Risk:</u> EPAS data is not shared external to the VA

<u>Mitigation:</u> EPAS data is not shared external to the VA

Section 6. Notice

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

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

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

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

SORN is currently being created.

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

SORN is currently being created.

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

Notice was transmitted to all users of the system.

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.

Users who require access to VistA are required to enter their Gender, SSN and DOB in order that account managers can properly create the necessary account. Declining to provide the necessary information to create an account will be cause the account to not be created and thus the individual would be denied access.

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.

By completing the EPAS workflow individuals consent to particular uses of the information. EPAS data is only used for the intent for which it was submitted.

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

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

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

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

<u>Principle of Use Limitation:</u> Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: Risk exist that users of EPAS may not receive notice from their management that sensitive personal information – including social security numbers, names, gender, date of birth and home addresses are stored. 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 result.

Mitigation: All VistA users are required to take ethics and cyber security in TMS annually. The application also provides built in safeguards to prevent the viewing of PII by unauthorized personnel.

Section 7. Access, Redress, and Correction

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

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

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

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

EPAS users can gain access to their information via the menu on the portal listed as "My Documents". The permission grants access to only the documents which they have created. Individuals can see the data including PII data they previously entered into the Workflow.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

N/A

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

An individual may gain access to his or her information by entering a ServiceNow ticket for assistance.

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.

Correcting EPAS information is accomplished via a ServiceNow ticket and routed to designated staff for correction. Individuals cannot directly correct their own data once the workflow is submitted.

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.

Each workflow includes instructions for correcting information. A notification email is sent to the individual regarding any change or correction.

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.

EPAS users are directed to use ServiceNow as the approved method to correct entries.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals***

involved might change their behavior. *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: Risk exist that an individual doesn't receive access to EPA

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, 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 Individual are provided with the ability to find out whether a project maintains a record relating to him. This is done by accessing the EPAS portal and searching "My Documents".
While access may be denied if deemed inappropriate by Subject Matter Experts (SME) responsible for the requested access area. Notice is given to user via email notification with instructions on what corrections are needed for the individual to change and resubmit.
EPAS uses the individuals network logon to prevent unauthorized use of information.

Section 8. Technical Access and Security

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

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

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

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

Individuals are granted access via their Network Logon to the EPAS system.
There are no users outside the VA with access to submit request using the EPAS system
EPAS users are granted permissions to EPAS workflows via active directory groups. Active Directory Security Group Owners review requests and approve them or send them back to the requestor for disposition or remediation.
Document Managers provide tier 3 support for individuals.

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

N/A

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.

System Admins – Creates and changes collections and permissions for all collections, Collection Admins – Creates and changes document types in a collection and permissions for those document types, Document Type Admins – Change a document type including routes and permissions, Users – Submits, Reviews and Completes workflows for particular documents

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.

Contractors will not have developer access to the system and PII.

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.

Privacy and Ethics training is provided through the Talent management System (TMS).

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Please provide response here
2. *The System Security Plan Status Date:* Please provide response here
3. *The Authorization Status:* Please provide response here
4. *The Authorization Date:* Please provide response here
5. *The Authorization Termination Date:* Please provide response here
6. *The Risk Review Completion Date:* Please provide response here
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Please provide response here

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

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

EPAS is in process for A&A and is under a 180-day ATO ending April 26, 2023.

Section 9 – Technology Usage

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

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

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

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

The system does not use Cloud computing.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

Cloud technology is not used for this system

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.

Cloud technology is not used for this system

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.

Cloud technology is not used for this system

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

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

No robotics automation is used in EPAS.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.08.08 08:23:39 -04'00'

Privacy Officer, Tonya Facemire

CRYSTAL WHITE

Digitally signed by CRYSTAL WHITE
Date: 2023.08.07 14:26:13 -04'00'

Information System Security Officer, Crystal White

RALEIGH MURRAY

Digitally signed by RALEIGH MURRAY
DN: c=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=People, cn=RALEIGH MURRAY, 0.9.2342.19200300.100.1.1=0003226791136001
Date: 2023.08.07 10:46:14 -05'00'

Information System Owner, Raleigh Murray

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).

A SORN is in development. The SORN for the system is currently in the process of being completed. The future SORN is Electronic Permissions Access System (EPAS)-VA (205VA005OPA31C)

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices