Privacy Impact Assessment for the VA IT System called:

Enterprise Precision Scanning and Indexing (EPSI)

Veterans Health Administration

Office of Integrated Veteran Care

eMASS ID # 1785

Date PIA submitted for review:

01/06/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Eller Pamintuan	eller.pamintuan@va.gov	303-331-7512
Information System Security Officer (ISSO)	Merle Kelley	merle.kelley@va.gov	319-430-7098
Information System Owner	Christopher Brown	christopher.brown@va.gov	202-270-1432

Abstract

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

The Enterprise Precision Scanning and Indexing (EPSI) web-based application will be used to streamline Veterans Affairs (VA) acceptance and temporary storage of Portable Document Format (PDF) records received from Office of Integrated Veteran Care (IVC) providers, to index them against a patient, and to transfer into the appropriate Veterans Health Information Systems and Technology Architecture (VistA) patient record for storage. PDFs received can contain all type of patient information, the individual patient health data is parsed out from PDF, it is attached, in whole, to patient's VistA record.

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 Enterprise Precision Scanning and Indexing (EPSI) web-based application will be sued to streamline Veterans Affairs (VA) acceptance and temporary storage of Portable Document Format (PDF) records received from Office of Integrated Veteran Care (IVC) providers, to index them against a patient, and to transfer them into the appropriate Veterans health Information Systems and Technology Architecture (VistA) patient record for storage. PDFs received can contain all type of patient information, the individual patient health data is not parsed out from PDF, it is attached, in whole, to patient's VistA record.

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.

Enterprise Precision Scanning and Indexing (EPSI) is sponsored by Health Information Management Service (HIMs) in conjunction with Office of Integrated Veteran Care (IVC) and is VA owned and operated. Yes the system has an eMASS entry.

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?

Potentially any Veteran receiving care through eternal IVC. Current volume is around 200k monthly submissions with information received from outside providers.

Check if Applicable	Demographic of individuals
☒	Veterans
☒	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?

EPSI is a web-based application used by VHA staff to attach PDF documents received from community providers to a patient's record in VistA Imaging.

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

The EPSI information system authenticates users using Single Sign-On Identification (SSOi) through Identity and Access Management (IAM) and use of a Secure Token Service (STS). The information received through IAM is also used in logging actions taken by users while within the EPSI information system (this creates non-repudiation within the EPSI information system). Corporate Data Warehouse (CDW) is used by EPSI to obtain information that will assist in identifying the records for document uploading into VistA. The EPSI information system also pulls information from CVIX for retrieval of patient information and sends information back to VIX for upload to VistA.

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

SSOi is applicable anytime a user accesses the system, CDW and CVIX are only applicable for information sharing in order to complete functionality in EPSI.

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?

The system only operates within VAEC AWS. As the system is hosted within the VA's cloud environment, it does not have any other site where PII is maintained. There are backups created within the cloud environment to ensure PII is maintained. The same controls are used for these backups as they are housed within the cloud environment.

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

H. What is the citation of the legal authority?

Refer to paragraph 3.H. below

Legal Authority: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.

Legal Authority: Title 38, United States Code, Sections 501(b) and 304.

Legal Authority: Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101.

Legal Authority: Title 38, United States Code, section 7301(a).

Legal Authority: Title 38, United States Code, sections 1710 and 1729.

I. What is the SORN?

SORN: 23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015), https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

SORN: 24VA10A7, Patient Medical Records - VA Care (Fee) Records - VA (10-02-2020), https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

SORN: 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015), https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf

SORN: 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12-23-2020), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

SORN: 114VA10, The Revenue Program-Billing and Collection Records - VA (1-25-2021), https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf

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, SORNs does not require amendment.

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, AWS Textract uses machine learning (ML) to review these documents and extract information needed. This means that it is analyzing the entire documents and not certain portions of it. Whatever information is on the documents will be analyzed/reviewed by Textract.

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
- ☐ Gender/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: Active Directory Name of System User, Consult Uniform Resources Name (URN), Medical Health Information, Security Identification (SecID), and Single Sign-On Identification (SSOI) Enumeration.

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?

All information is received from CDW, CVIX, and documents uploaded to EPSI by VA user.

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 patient's name is then input into an Application Program Interface call (API) to VistA Imaging Exchange (VIX) that retrieves the list of available patients at that site that match the name pattern. The staff user using the EPSI web-based application is then required to select a patient prior to continuing the workflow. After a patient is selected, the patient's Integration Control Number (ICN) has been identified and is then held in local memory on the web-browser.

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

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

The EPSI system does not create information.

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?

Information is collected from the documents the VA staff member are processing. Information is also collected from the VistA Exchange using Application Program Interface Calls (API).

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?

EPSI does not collect information on forms.

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.

Information is checked for accuracy in three ways within the EPSI web-based application.

Patient Search: Patient selection accuracy is assured by providing the staff EPSI user with the last four digits of the social security number, in addition to the patient's full name and date of birth.

Consult Information: The consult information is validated by retrieving the patient's ICN from the selected result of the patient search request.

Data Confirmation Screen: All users selected, or input information is displayed on a data confirmation screen prior to uploading the data to the patient record for accuracy.

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?

There is no commercial aggregator involved. Confirmation screen does show and provide a verification point, but there are no external interfaces used for validation.

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

SORN: 23VA10NB3, *Non-VA Care (Fee) Records* - VA (7-30-2015), https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

Legal Authority: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.

SORN: 24VA10A7, *Patient Medical Records* - VA *Care (Fee) Records* - VA (10-02-2020), https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

Legal Authority: Title 38, United States Code, Sections 501(b) and 304.

SORN: 54VA10NB3, *Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files* - VA (3-3-2015), https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf

Legal Authority: Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101.

SORN: 79VA10, *Veterans Health Information Systems and Technology Architecture (VistA) Records* - VA (12-23-2020), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

Legal Authority: Title 38, United States Code, section 7301(a).

SORN: 114VA10, *The Revenue Program-Billing and Collection Records* - VA (1-25-2021), https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf

Legal Authority: Title 38, United States Code, sections 1710 and 1729. ADD ANSWER HERE

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: Personally Identifiable Information of a Veteran may not be accurate, complete, and current in the system.

Mitigation: EPSI web-based application system relies on the source of internal connection systems such as VistA Exchange and VistA Imaging to ensure that personally identifiable information (PII) is accurate, complete, and current.

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
Date of Birth	Ensuring correct Veteran's medical records is	Not used

	presented/selected and updated.	
Social Security Number (Last Four)	Ensuring correct Veteran's medical records is presented/selected and updated.	Not used
Name	Ensuring correct Veteran's medical records is presented/selected and updated.	Sent to CVIX for patient retrieval.
Integration Control Number	Ensuring correct Veteran's medical records is presented/selected and updated.	Sent to CVIX for consult retrieval.
Medical Records	Used for Indexing.	Sent to VistA for Indexing.
Medical Health Information.	Used for Indexing.	Sent to VistA for Indexing
Consult Uniform Resource Name (URN)	Ensuring correct Veteran's medical records is presented/selected and updated.	Sent to CVIX for consult retrieval.
Active Directory Name of System User	Used for SSOi.	VA IAM/SSOi.
Security Identification (SecID) Single Sign-On Identification (SSOI) Enumeration	Used for SSOi.	VA IAM/SSOi.

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?

Currently, data analytics is not part of the EPSI web-based application, and no analytics-based results are produced.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The EPSI information system receives PDFs from consults and provides this information to users to either update or create new medical records of patients. Any information retrieved from the Intelligent Document Processing process that is not needed or used during the processing of the record to VistA will not be accessible to Government employees and all data will be deleted after 30 days.

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?

The information in the EPSI web-based application is secured by encrypting data in transit and at rest.

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

Yes, data are encrypted

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

To transmit data securely, data in transit is encrypted using FIPS-140-2 encryption (certificate#: 1747 –OpenSSL encryption, 3139). To the extent possible, data in transit is passed between services inside of the Virtual Private Cloud (VPC) within Amazon Web Services (AWS) Gov.

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?

Access to PII is limited by the EPSI application to only those data items deemed necessary for an Indexer to perform their job, as determined by their management team and their job description.

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?

System documentation includes detailed system design and user guides that specify those areas of the system that contain PII and PHI, as well as how it is to be used by the Indexers/VA Personnel. Additionally, user roles are implemented to restrict user's access to only the specific information required to perform their job function. Roles within the system are determined and requested by Business Unit supervisors (Senior Program Analyst or higher).

2.4c Does access require manager approval?

User access is provided by VA IAM/SSOi System Administrators following receipt of request from appropriate manager/supervisor

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

Yes, access is tracked through logging of view requests available in log files with tokens indicating the user who is requesting access to view and edit system information.

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

The EPSI application implements auditing which tracks user access to the system and all data accessed. The information is mapped in the audit record by VA/EPSI agent identifier and Veteran identifier used for data access.

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*

EPSI retains Social Security, Date of Birth, Medical Records, Consult Uniform Resource Name (URN) and Medical Health Information for 30 days.

This data is in the form of PDFs that have been uploaded by the user and the data is used for reporting and to enable a QA workflow for the business. Security Identification (SecID) is retained by EPSI for tracking user sessions and tying logs of user interactions.

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.

Records that have been successfully uploaded and that are attached to a patient / Consult Uniform Resource Name are held for 30 days to allow for auditing (ensuring the documents have been uploaded to the correct patient record)

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?

EPSI is not a system of record, it is a passthrough of data from VistA acting as a primary workflow application that provides VHA staff the ability to upload files to patient's record in VistA Imaging. Interim electronic information is compiled, as noted in 6000.2, Destroy/delete after migration of information to another electronic medium. Destruction of interim version of information is not to occur until it has been determined that the migrated information represents an exact duplicate of the previous version of the migrated information. N1-15-02-3, Item 2 https://www.va.gov/VHApublications/RCS10/rcs10-1.pdf

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

VHA records control schedule 10-1; https://www.va.gov/VHApublications/RCS10/rcs10-1.pdf Item #1260.1. g. Electronic Indexes, Indexes used to provide access to electronic files. Disposition: Temporary, delete when related files are no longer needed. Authority: N1-15-03-1, item 6.

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.

PDF documents that potentially contain SPI are stored in binary format and overwritten with null values from the system 30 days after a successful upload. The PDF documents are converted into a database storage friendly format. Consult history is retrieved from CDW, but not stored in the EPSI database. The information is only stored in local memory as a variable with a scope only relevant to that particular indexing action. Any potential SPI stored in the consult history that is retrieved for ensuring the correct consult has been applied, is not stored, nor cached, and is automatically overwritten with null values from the system upon successful upload, or selection of a new document or patient.

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.

The EPSI web-based application has built out a robust set of test data to include test patients and consults, it does not utilize any PII for training, or testing. PII is sometimes utilized during the research process. In order to minimize the risk to privacy the EPSI team attends monitored, non-recorded, sessions with VA employees and stakeholder to observe current business processes. EPSI team member are not authorized to record, retain, or distribute this data in any fashion.

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: The risk that Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) may be breached increases the longer their information is retained.

Mitigation: To combat the risk of PII and other SPI breached. The EPSI web-based application system incorporates encryption and secure data transfer protocols and features. Local variables that are utilized during the matching of the document to the patient get populated from API calls to VIX or CDW. In order to provide the staff user with the information required to ensure the patient and linked appointment (consult) has been correctly identified. These variables are overwritten with null values as soon as they come out of scope for the workflow. Such as, a user clicks back to exit the workflow or submit to upload the record. PII that is no longer relevant to the UI is overwritten with null values at the end of the user workflow where it is relevant, or immediately if it is not relevant. PII such as patient ICN, Consult Uniform Resource Name, and Patient name used for uploading the document and subsequent auditing, are purged after 30 days per the business requirements. The purge process is triggered when the following happens: 30 days after the system successfully matched to a patient and uploaded into a record. The documents are then removed via an automated process, where the information is overwritten with null values.

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. Enterprise Precision Scanning and Indexing consists of 4key 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 <**Information System Name**> 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	**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**

(API) etc.) that contains PII/PHI					
EPSI database	Yes	Yes	Integration Control Number, Name, Date of Birth, Social Security Number, Medical Health Information, Medical Records	Used to identify the record for document uploading and auditing	Stored in encrypted Amazon Rational Database Service (RDS) Aurora and data is destroyed by deletion after 30 days.
Community Care EPSI database	Yes	Yes	Integration Control Number, Consult Uniform Resource Name	Used to identify the record for document uploading and auditing	Information provided is housed in CDW and has the controls associated with that service.
AWS S3 idp-input	Yes	Yes	Integration Control Number, Name, Date of Birth, Social Security Number, Medical Health Information, Medical Records	Used to gather information from the fax submitted to EPSI to link to VistA and provide information Ingest the submitted fax to prepare for processing.	Encrypted at rest with key AES-256, encrypted in motion (in transit), Data is destroyed after 30 days by deletion.
AWS S3 idp-output	Yes	Yes	Name, Date of Birth, Medical Health Information	Used to gather information from the fax submitted to EPSI to link to VistA and provide	Encrypted at rest with key AES-256, encrypted in motion (in transit),

				information. Output the results from IDP workflow to initiate function to send to UI.	Data is destroyed after 30 days by deletion.
Amazon Web Service Textract	Yes	Yes	Integration Control Number, Name, Date of Birth, Social Security Number, Medical Health Information, Medical Records	Used to gather information from the fax submitted to EPSI to link to VistA and provide information.	Encrypted at rest with key AES-256, encrypted in motion (in transit), Data is destroyed after 30 days by deletion.

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***
Veterans Health Administration (VHA) Corporate Data Warehouse (CDW)	Correctly indexing the received records with the accurate EHR data	Social Security Number (SSN), Date of Birth, Integration Control Number, Medical Health Information, Consult Uniform Resource Name (URN), Medical Records Name	HTTPS Data in transit is encrypted using FIPS-140-2 encryption (OpenSSL encryption, 1433)
Veterans Health Administration (VHA) Vista/ VistA Link/ VIX	Connecting to the appropriate VISTA using authenticated credentials	Integration Control Number (ICN), Consult Uniform Resource Name (URN), Social Security Number (SSN), Medical Health Information, Medical Records	HTTPS Data in transit is encrypted using FIPS-140-2 encryption (certificate#: 1747 – OpenSSL encryption, 3139)
Veterans Health Administration (VHA) Identity and Access Management (IAM) SSOi	The VHA IAM service SSOi is used to provide internal single sign on and identify and access management within the VA network, for VA employees	Active Directory Name of System User, Security Identification (SecID)	HTTPS Data in transit is encrypted using FIPS-140-2 encryption (certificate#: 1747 – OpenSSL encryption, 3139)
Veterans Health Administration (VHA) Identity and Access Management (IAM) SSOi -provisioning	The VHA IAM service SSOi is used to provide internal single sign on and identify and access management within the VA network, for VA employees	Active Directory Name of System User, Security Identification (SecID) Single Sign-On Identification (SSOI) Enumeration	HTTPS Data in transit is encrypted using FIPS-140-2 encryption (certificate#: 1747 – OpenSSL encryption, 3139
Veterans Health Administration (VHA)	The VHA IAM service SSOi is used to provide internal single sign on	Integration Control Number, Name, Date of Birth, Social Security Number, Medical	HTTPS Data in transit is encrypted using

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*
Identity and Access Management (IAM) SSOi - STS (Secure Token Service)	and identify and access management within the VA network, for VA employees	Health Information, Medical Records	FIPS-140-2 encryption (certificate#: 1747 – OpenSSL encryption, 3139)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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 risk that information may be accessed by an unauthorized VA personnel without a need to know.

Mitigation: System is only available to authorized VA personnel. These users would need to have a VA PIV card, access to the VA network, a valid VistAID for the site they are trying to access, in addition to a request approved by that site's administrator via the Identity and Access Management (IAM)– Single Sign-On Internal (SSOi) provisioning process. SSOi validates user's account against PIV/Windows Active Directory authentication. All access is monitored, traced, and logged. User access and activity is logged in the EPSI database. API calls including the document retrieval are secured by SSOi headers via a JSON web token. Upon login, the SSOi systems will send a SECID header to the EPSI web-based application. This header is the unique identifier for the user in the VA SSOi system and is used as a unique identifier for users within the EPSI web-based application. The EPSI web-based application will then lookup that user by SECID and return the retrieved user / site information to the browser via a JSON web token. This web token will contain the information required to ensure the user has access to the system and role-based authorization to use that endpoint. Example: to retrieve the PDF document list, only authorized users at a site with the indexer role can view, but the QA personnel roles are not authorized access.

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***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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: The web-based application does not receive or send information outside of the VA.

Mitigation: The web-based application does not receive or send information outside of 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 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.

It is Veterans Health Administration (VHA) policy that the VHA Notice of Privacy Practices (Information Bulletin 10-163) is created, maintained, and distributed in compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule at 45 C.F.R. § 164.520, to inform Veterans, beneficiaries, caregivers, and non-Veteran patients of the use and disclosure of their health information without authorization, their rights to access and restrictions on certain uses and disclosures and VHA's legal duties to maintain the privacy of their health information. AUTHORITY: 45 C.F.R. parts 160 and 164.

VHA Notice of Privacy Practices is located at https://www.va.gov/files/2022-10/10-163p_%28004%29_-Notices_of_Privacy_Practices-_PRINT_ONLY.pdf.

6.1b If notice was not provided, explain why.

Notice is not provided by the EPSI system as the EPSI system itself does not collect data directly from patients.

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

The system does not collect information from individuals. The Sources collecting the information provide this notice.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

VHA Directive 1605.1, Privacy and Release of Information, paragraph 5, lists the Individuals' Rights of the Veterans and Beneficiaries to request VHA to restrict the use and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. Veterans have the right to refuse to disclose their SSNs to VHA. The individual is denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (please refer to the: 38 Code of Federal Regulations CFR 1.575(a)).

If the Veterans or Beneficiaries does not wish to provide their SSN, they may provide their EDIPI. Alternatively, they may provide their First Name, Last Name, and Date of Birth. If the stakeholder does not wish to provide any of this information, there is no denial of service; however, the employee will be unable to assist the stakeholder.

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 VA's Notice of Privacy Practices describes how an individual can exercise their right of consent for use of information and how to exercise this right.

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: If notice is not provided in a timely manner, an individual may give information that they do not want to be shared.

Mitigation: The EPSI information system does not collect information directly from an individual, and the mitigation is not applicable for the EPSI information system and is the responsibility of the VA to provide the privacy practice notices to the Veteran at the time of service in accordance with VHA Handbook 1605.4 NOTICE OF PRIVACY PRACTICES

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.***

VHA Directive 1605.01: Privacy and Release of Information states the rights of Veterans and Beneficiaries to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review or seek copies of records must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access to data must be delivered to, and reviewed by, the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must include the signature

of the requester, date of birth, copy of signed government identification, state what is request and the period of the information requested. Mail requests for eligibility information/records to: CHAMPVA Eligibility PO Box 469028 Denver, CO 80246-9028. Mail requests for CHAMPVA billing/claim records to: VHA Office of Integrated Veteran Care Privacy/FOIA Office, PO Box 469060 Denver, CO 80246-9060. Requests for medical and pharmacy records contact your servicing medical provider and for Community Care authorizations/authorization numbers are located at the referring VA Medical Center. For Veteran claim payment information will need to be submitted to the VA Financial Services Center (FSC) Privacy Office by first contacting them via email at vafscprivacyofficer@va.gov for secure submission methods. For Veteran Explanation of Benefits maintained by the VA's Third-Party Administrators may be requested by the Veteran registering and requesting their records from either (TriWest Healthcare Alliance) (https://veteran.triwest.com/bizflowappdev/apps/veteranportal/?tz=GMT-0700 or Optum (https://veteran.vacommunitycare.com/start). Medical and pharmacy records should be sought from the medical facility where the patient received care and Veteran and Beneficiary (CHAMPVA) lien or subrogation requests should be submitted to the respective action office via the instructions located at https://www.va.gov/OGC/Collections.asp.

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)?

The system does not collect information from individuals. The Sources collecting the information provide this notice. Individuals have the rights to request access to review their records by submitting the VHA-10-5345 provides the process to Request for and Authorization to Release Medical Records or Health Information.

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?

The system does not collect information from individuals. The Sources collecting the information provide this notice. Individuals have the rights to request access to review their records by submitting the VHA-10-5345 provides the process to Request for and Authorization to Release Medical Records or Health Information.

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.

Veterans and beneficiaries have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request must be mailed or delivered to the organization that maintains the record. A request for amendment of information contained in a system of records

must be delivered to the System Manager, or designee, for the concerned system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans and beneficiaries may request changes to their information in accordance with VHA Handbook 1605.1, paragraph 5 states the rights of veterans and beneficiaries to amend their records by submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, which may be used as the written request requirement. This includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.57.

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.

If a Veteran or Beneficiary discovers that incorrect information was provided during the intake process, they must submit an information amendment request. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

7.5 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: If an individual discovers the VHA Office of Community Care has incorrect information on them, or an address or life event update. There is a risk that incorrect information is accidentally recorded in an individual's record. An individual may want to review the content of their record to check for data accuracy. The magnitude of harm associated with this risk to the VA is low.

Mitigation: Individuals have a right to contact the VHA call center to gain access to their information. In addition, authentication of data is in place to safeguard against incorrect information being loaded. An individual who wishes to determine whether a record is being maintained in this system under their name or other personal identifier, or who wants to review the contents of such a record, should submit a written request. Inquiries should include the patient's full name, SSN, and return address.

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?

The supervisor/Contracting Officer's Representative (COR) documents and monitors individual information system security training activities, including basic security awareness training and specific information system security training. This documentation and monitoring is performed through the use of the Talent Management System (TMS). Access to the system is granted to VA employees and contractors the supporting IT for the application after the supervisor/COR authorizes this access once requirements have been met. Only the IT system administrators authorized by VA IT will have the security role to modify the application. This PIA will not result in technology protocol changes, additional controls, or single sign on, as per privacy control AR-7, Privacy-Enhanced System Design and Development.

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?

No other agencies are allowed access to EPSI.

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.

Developer Access: Developers account management processes should further ensure that only end users are able to access the environment. Developers and EPSI Project teams will work to create, update, access and disable developer accounts for project teams. Additionally, there shall be a review of user access periodically to evaluate whether users are active in the environment; if the user is not active, their account is terminated. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. A designated VA Project Point of Contact (POC) is the only person who may submit account creation requests and submitted for accountability purposes.

End-User and Tester Access: All individuals requesting developer access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203)) and applicable role-based training. This may include but is not limited to Information Security for IT Specialists Training) and must be authorized by VA Project Manager. To ensure that this requirement is met, the designated VA Project POC must submit a signed Access Request Form for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access to the EPSI application Environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, current on VA Training, VA Employee or Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date, access justification and completed training certifications.

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.

Each contractor must sign an NDA. Contracts are reviewed by the COR at the time of each period of performance specified within the contract. Contractors will only have access to PII that is required in order to do their job. This may be required to assist users with functionality of the system or to ensure the system is functioning appropriately.

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

Yes, the contractor will have access to PII.

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

Yes, the contractor will have access to PII. VA contractors have access to the pre-production environments for development purposes. Contractors also have access to the live production system for maintenance activities.

8.2c. Does the contractor have a signed confidentiality agreement?

All contractors must sign an NDA.

8.2c. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

A BAA has been completed for the contract.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
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.

The following steps are required before contractors can gain access to the system:

•Contractors must take and pass training on VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA10203), and government ethics and role-based training based on support role to the system.

•Contractors must have signed the Non-Disclosure Agreement (NDA) and Rules of Behavior (RoB).

•Contractors must have successfully completed VA contractor background security investigation as per the Position Designation Automated Tool (PDT).

•Once complete, a request is submitted for access. Before access is granted to the production environment; this request must be approved by the supervisor, and OIT.

VA owns the data that the EPSI application extracts from the source applications and secures the EPSI application data. The VA and CORs have weekly meetings for the review of the contract details and this contract is reviewed at least on an annual basis. There shall be a regular review of user access to evaluate whether users are active in the environment. If a user is not active, the account will be terminated. A designated VA Project POC is the only person who may submit account creation requests for accountability purposes. Contractor access to the system expires at the end of the contract duration or earlier.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

•VA 10176: Privacy and Info Security Awareness and Rules of Behavior
•VA 10203: Privacy and HIPPA Training
•VA 3812493: Annual Government Ethics Role-based Training includes but is not limited to and based on the role of the use
•VA 1016925: Information Assurance for Software Developers IT Software Developers
•VA 3193: Information Security for CIOs Executives, Senior Managers, CIOs and CFOs
•VA 1357084: Information Security Role-Based Training for Data Managers
•VA 64899: Information Security Role-Based Training for IT Project Managersst
•VA 3197: Information Security Role-Based Training for IT Specialists
•VA 1357083: Information Security Role-Based Training for Network Administrators
•VA 1357076: Information Security Role-Based Training for System Administrators
•VA 3867207: Information Security Role-Based Training for System Owners

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

8.4a If completed, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 11/03/2023
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* 05/14/2024
5. *The Authorization Termination Date:* 05/14/2026
6. *The Risk Review Completion Date:* 04/11/2024
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.***

Not Applicable

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)***

The EPSI web-based application system is hosted by the VA Enterprise Cloud (VAEC) AWS and is identified as an IaaS.

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.*

Not Applicable, reference paragraph 9.1.

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.

Not Applicable, reference paragraph 9.1.

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.

Not Applicable, reference paragraph 9.1.

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).

The EPSI information system will be using AWS Textract through the VAEC AWS offerings. The Artificial Intelligence/Machine Learning will be part of the Intelligent Document Processing process, specifically AWS Textract, will be used for Optical Character Recognition (OCR), signature detection, and queries to identify information off of the faxed medical records.

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 provided in this Privacy Impact Assessment is true and accurate.

ELLER PAMINTUAN

Digitally signed by ELLER PAMINTUAN
Date: 2025.01.27 14:24:52 -07'00'

Privacy Officer, Eller Pamintuan

MERLE KELLEY

Digitally signed by MERLE KELLEY
Date: 2025.01.28 09:56:24 -06'00'

Information Systems Security Officer, Merle Kelley

CHRISTOPHER BROWN

Digitally signed by CHRISTOPHER BROWN
Date: 2025.01.28 13:35:20 -06'00'

Information Systems Owner, Christopher Brown

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; screen shot of a website collection privacy notice).

Department of Veterans Affairs, Veterans Health Administration, Notice of Privacy Practices

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)