Privacy Impact Assessment for the VA IT System called:

Enterprise Precision Scanning and Indexing (EPSI)

Veterans Health Administration

Office of Integrated Veteran Care

Date PIA submitted for review:

09/15/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michael Hartmann	Michael.Hartmann@va.gov	303-780-4753
Information System Security Officer (ISSO)	Merle Kelley	Merle.Kelley@va.gov	319-430-7098
Information System Owner	Christopher Brown	Christopher.Brown1@va.gov	202-270-1432

Abstract

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

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 them into the appropriate Veterans Health Information Systems and Technology Architecture (VistA) patient record for storage. PDFs received can contain all types of patient information, the individual patient health data is not parsed out from PDF, it is attached, in whole, to patient's VistA record.

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.

Enterprise Precision Scanning and Indexing (EPSI). Office of Integrated Veteran Care (IVC)

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

EPSI will be rolled out nationally to be used in all medical centers and will only be accessible on the VA network. Users will authenticate for access using Identity and Access Management (IAM) Single Sign-On Internal (SSOi) and be authorized within the system for their role. All information transfers will be secure over a secure socket layer (SSL) connection and data stored in an encrypted database. There is no permanent PII/PHI information stored in the database. Any PHI will be contained on the faxed documents and not parsed out of the document. The faxed documents will only be stored temporarily and will be deleted from EPSI 30 days after it is transferred to VistA Imaging.

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

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. 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.

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.

Potentially any Veteran receiving care through external IVC. Current volume is around 100k monthly individual encounters with information received from outside providers.

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

The patient's name and date of birth is collected from the documents the VA staff member are processing. The patient's name is then input into an Application Program Interface call (API) to Centralized VistA Imaging Exchange (CVIX) 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. The EPSI web-based application then takes the patient's ICN and passes it back to CVIX to retrieve the available consult for a patient. The staff user using the EPSI web-based application is then prompted to select a consult and the Consult Uniform Resource Name (URN) is held in local memory on the web-browser. After the remaining non-PII related steps are completed, the user places the document, Patient ICN, and Consult Uniform Resource Name (URN) in a que to be processed by VIX, then uploading it to the patient record. Other than the patient, internal systems such as VistA Imaging Exchange (VIX) are required in the process because the document is being uploaded without the patient present.

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

EPSI will not be a system of record. There is no permanent storage of PII or patient information.

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.

EPSI will not be a system of record. There is no permanent storage of PII or patient information.

3. Legal Authority and SORN

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

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) - VA (12-23-2020)
114VA10, The Revenue Program-Billing and Collections Records - VA (1/25/2021)
26 U.S. Code § 61 – Gross Income Defined (a) (12) Income from Discharge of Indebtedness
38 U.S. Code § 31 – Foreign Medical Program
38 U.S. Code § 304 – Deputy Secretary of Veterans Affairs

38 U.S. Code § 501 – Veterans' Benefits Rules and Regulations
38 U.S. Code § 1151 – Benefits for Persons Disabled by Treatment or Vocational Rehabilitation
38 U.S. Code § 1703 – Contracts for Hospital Care and Medical Services in Non-Department Facilities
38 U.S. Code § 1710 – Eligibility for Hospital, Nursing Home, and Domiciliary Care
38 U.S. Code § 1720G – Assistance and Support Services for Caregivers
38 U.S. Code § 1724 – Hospital Care, Medical Services, and Nursing Home Care Abroad
38 U.S. Code § 1725 – Reimbursement for Emergency Treatment
38 U.S. Code § 1728 – Reimbursement of Certain Medical Expenses
38 U.S. Code § 1729 – Recovery by the United States of the Cost of Certain Care and Services
38 U.S. Code § 1741 – 1743 – Per Diem Grant – State Home
38 U.S. Code § 1781 – Medical Care for Survivors and Dependents of Certain Veterans
38 U.S. Code § 1786 – Care for Newborn Children of Women Veterans Receiving Maternity Care
38 U.S. Code § 1787 – Health Care of Family Members of Veterans Stationed at Camp Lejeune, North Carolina
38 U.S. Code § 1802 – Children of Vietnam Veterans Born with Spina Bifida – Spina Bifida Conditions
38 U.S. Code § 1803 – Children of Vietnam Veterans Born with Spina Bifida – Health Care
38 U.S. Code § 1812 – Children of Women Vietnam Veterans Born with Certain Birth Defects, Covered Birth Defects
38 U.S. Code § 1813 – Children of Women Vietnam Veterans Born with Certain Birth Defects, Health Care
38 U.S. Code § 1821 – Benefits for Children of Certain Korea Service Veterans Born with Spina Bifida
38 U.S. Code § 3102 – Basic Entitlement – A Person Shall be Entitled to a Rehabilitation Program
38 U.S. Code § 5701 – Confidential nature of claims
38 U.S. Code § 5724 – Provision of Credit Protection and Other Services
38 U.S. Code § 7301 – Functions of Veterans Health Administration: in general
38 U.S. Code § 7332 – Confidentiality of Certain Medical Records
38 U.S. Code § 8131 – 8137 – Construction Grant – State Home
44 U.S. Code § – Public Printing and Documents
38 CFR 2.6 – Secretary's delegations of authority to certain officials (38 U.S.C. 512)
45 CFR Part 160 – General Administrative Requirements
45 CFR Part 164 – Security and Privacy
Public Law 103 – 446, Section 107. Veterans Education and Benefits Expansion Act of 2001 – Section 107. Expansion of Work-Study Opportunities
Public Law 111 – 163 Section 101. Caregivers and Veterans Omnibus Health Services Act of 2010 – Section 101. Assistance and Support Services for Caregivers
Public Law 115 - 26 - An act to amend the Veterans Access, Choice, and Accountability Act of 2014 to modify the termination date for the Veterans Choice Program, and for other purposes

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?*

System is not modified and SORNs do not require amendment.

D. System Changes

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

Completion of this PIA will not result in circumstances that require changes to business processes.

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

Completion of this PIA will result in the upgrade of Hyperscience from V34 to V36.

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)

Consult Uniform Resource Name (URN), Active Directory Name of System User, Security Identification (SecID) Single Sign-On Identification (SSOI) Enumeration, Medical Health Information.

PII Mapping of Components (Servers/Database)

EPSI web-application consists of three key components. The EPSI database component and the Corporate Data Warehouse (CDW) component. The components have been analyzed to determine if any elements of that component collect PII. The type of PII collected by EPSI 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
epsi_db	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 overwriting with null values after 30 days.
cc_epsi	Yes	Yes	Integration Control Number, Consult	Used to identify the record for document	Information provided is housed in the Corporate Data

			Uniform Resource Name	**uploading and auditing**	**Warehouse and has the controls associated with that service.**
Hyperscience (epsi-prod-hs-db)	**Yes**	**No**	**Name, Date of Birth**	**Used to identify the correct patient and record for document uploading and auditing**	**Our current version of Hyperscience (V34) is TRM approved HyperScience (va.gov) EPSI will be moving to Hyperscience (V36) with approval of the PIA. TRM review is in process and a POAM is in place until TRM approval has been received.** **Data is encrypted at disk** **PII Data retention policy of 30 days is compliant with VA mandates**

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

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

The patient's name and date of birth is collected from the documents the VA staff member are processing.

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.

1.2c If the system creates 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 How is the information collected?

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

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

Information is collected 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, give the form's OMB control number and the agency form number.

Information is collected from interfaces where the data can be validated. However, no additional forms are produced requiring an OMB Control number.

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

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

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

Information is checked for accuracy 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 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.

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 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

Systems of Records Notices: https://www.oprm.va.gov/privacy/systems_of_records.aspx
23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) - VA (12-23-2020)
114VA10, The Revenue Program-Billing and Collections Records - VA (1/25/2021)
26 U.S. Code § 61 – Gross Income Defined (a) (12) Income from Discharge of Indebtedness
38 U.S. Code § 31 – Foreign Medical Program
38 U.S. Code § 304 – Deputy Secretary of Veterans Affairs
38 U.S. Code § 501 – Veterans' Benefits Rules and Regulations
38 U.S. Code § 1151 – Benefits for Persons Disabled by Treatment or Vocational Rehabilitation
38 U.S. Code § 1703 – Contracts for Hospital Care and Medical Services in Non-Department Facilities
38 U.S. Code § 1710 – Eligibility for Hospital, Nursing Home, and Domiciliary Care
38 U.S. Code § 1720G – Assistance and Support Services for Caregivers
38 U.S. Code § 1724 – Hospital Care, Medical Services, and Nursing Home Care Abroad
38 U.S. Code § 1725 – Reimbursement for Emergency Treatment
38 U.S. Code § 1728 – Reimbursement of Certain Medical Expenses
38 U.S. Code § 1729 – Recovery by the United States of the Cost of Certain Care and Services
38 U.S. Code § 1741 – 1743 – Per Diem Grant – State Home
38 U.S. Code § 1781 – Medical Care for Survivors and Dependents of Certain Veterans
38 U.S. Code § 1786 – Care for Newborn Children of Women Veterans Receiving Maternity Care
38 U.S. Code § 1787 – Health Care of Family Members of Veterans Stationed at Camp Lejeune,

North Carolina
38 U.S. Code § 1802 – Children of Vietnam Veterans Born with Spina Bifida – Spina Bifida Conditions
38 U.S. Code § 1803 – Children of Vietnam Veterans Born with Spina Bifida – Health Care
38 U.S. Code § 1812 – Children of Women Vietnam Veterans Born with Certain Birth Defects, Covered Birth Defects
38 U.S. Code § 1813 – Children of Women Vietnam Veterans Born with Certain Birth Defects, Health Care
38 U.S. Code § 1821 – Benefits for Children of Certain Korea Service Veterans Born with Spina Bifida
38 U.S. Code § 3102 – Basic Entitlement – A Person Shall be Entitled to a Rehabilitation Program
38 U.S. Code § 5701 – Confidential nature of claims
38 U.S. Code § 5724 – Provision of Credit Protection and Other Services
38 U.S. Code § 7301 – Functions of Veterans Health Administration: in general
38 U.S. Code § 7332 – Confidentiality of Certain Medical Records
38 U.S. Code § 8131 – 8137 – Construction Grant – State Home
44 U.S. Code § – Public Printing and Documents
38 CFR 2.6 – Secretary's delegations of authority to certain officials (38 U.S.C. 512)
45 CFR Part 160 – General Administrative Requirements
45 CFR Part 164 – Security and Privacy
Public Law 103 – 446, Section 107. Veterans Education and Benefits Expansion Act of 2001 – Section 107. Expansion of Work-Study Opportunities
Public Law 111 – 163 Section 101. Caregivers and Veterans Omnibus Health Services Act of 2010 – Section 101. Assistance and Support Services for Caregivers
Public Law 115 - 26 - An act to amend the Veterans Access, Choice, and Accountability Act of 2014 to modify the termination date for the Veterans Choice Program, and for other purposes

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

The patient information in the EPSI web-based application will be used as followed:

- Transient information (not stored): Date of Birth, Social Security Number (Last Four)
- Stored Information: Name, Integration Control Number

The Integration Control Number is passed by EPSI to VIX during the document upload and is used to identify the correct patient record to add the file to. This information will help support the program's business purpose by providing the ability for clinical documents, including consult result documents from community providers to be managed through a standardized process and automatically incorporated in a Veterans Electronic Heath Record (HER) after the Office Integrated Veteran Care (IVC) and Health Information Management Service (HIMs) review.

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.

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.

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

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?

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?

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.

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

To hold data securely, data at rest is stored in an encrypted Amazon RDS (Relational Database Services) (postgres) database.

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?

Eligibility for access to the PII displayed by the EPSI web-based application is determined by ensuring a staff user has VA Access (SSOi authentication) and VistA access (VistAID SSOi headers).

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

Yes, all procedures, controls and procedures are documented.

2.4c Does access require manager approval?

Authorization for the access is requested by the users through the SSOi provision process. Requests for access are routed to 2 approvers responsible for ensuring appropriate access by site.

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?

VHA ensures that the practices stated in the PIA are reinforced by requiring Contractors and VA employees to complete all VA trainings including VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203). Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply. Through TMS employees and contractors are monitored, CORS are responsible for ensuring assignment in TMS training. Training audits occur monthly and are conducted by ISSOs throughout the VA. Training records are stored in the TMS system. Any user who is not current in Privacy/Infosec training loses access to all VA data until they become current on required training. All incidents are required to be reported to the supervisor or

ISSO / Privacy Officer within 1 hour of occurrence. If the ISSO determines a security event has occurred, they open a PSETS ticket and inform CSOC and DBRS. Credit monitoring may be provided to any person whose sensitive information has been violated, and the system user who put the data at risk will be retrained and consequences of actions up to loss of job.

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 together.

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.*

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA Records Officer will assist in providing a proposed

schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. This question is related to privacy control DM-2, Data Retention and Disposal.

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

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, and the information is destroyed every 30 days.

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

EPSI follows VHA Records Control Schedule (RCS 10-1) https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf . Item number 6000.2 Electronic Health Record (EHR). Electronic Health Records (EHR). Records Description: Interim Electronic Source Information. Electronic version of source information obtained from other electronic databases, optical disk, or other magnetic media not considered as part of the consolidated patient medical record. May include information generated electronically by medical equipment. Disposition Instructions: Temporary. 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. Disposition Authority: N1-15-0203, Item 2.

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 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: 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.

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***
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) Identity and Access Management (IAM)	The VHA IAM service SSOi is used to provide internal single sign on and identify and access management within the VA	Integration Control Number, Name, Date of Birth, Social Security Number, Medical Health Information, Medical Records	HTTPS Data in transit is encrypted using FIPS-140-2 encryption (certificate#: 1747 – OpenSSL encryption, 3139)

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*
SSOi - STS (Secure Token Service)	network, for VA employees		

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: 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 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	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.

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

Follow the format below:

Privacy Risk: N/A, the web-based application does not receive or send information outside of the VA.

Mitigation: N/A, 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 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.

The data collection from the individual in this workflow has already happened outside of the EPSI web-based application system from other VA systems. No new data is collected from individuals.

Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES
23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) - VA (12-23-2020)
114VA10, The Revenue Program-Billing and Collections Records - VA (1/25/2021)

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

Information is not collected directly from the patients.

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.

Authority to collect is stated in the following SORNs:
23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) - VA (12-23-2020)
114VA10, The Revenue Program-Billing and Collections Records - VA (1/25/2021)

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.

Information is not collected directly from the patients. Staff users collect data from the documents pending upload in order to correctly identify the patient's record and consult the document should be added to. The data collection from the individual in this workflow has already happened outside of the EPSI web-based application system.

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.

Information is not collected directly from the patients. Staff users collect data from the documents pending upload in order to correctly identify the patient's record and consult the document should be added to. The data collection from the individual in this workflow has already happened outside of the EPSI web-based application system. Therefore, there is no need or mechanism to request consent from the patient to attach the document to their medical record.

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 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 Transparency: Has sufficient notice been provided to the individual?

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

Privacy Risk: 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 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.***

An individual can, at any time, request their health records through existing MyHealtheVet or other VA programs external to the EPSI web-based application. The EPSI web-based application processes documents to attach the health record with the ultimate goal that the patients and providers can get them back when the health record is retrieved or accessed.

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).

EPSI is not a system of record.

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.

EPSI is not a system of record.

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.

Incorrect information, such as a document being uploaded to the wrong record, must be corrected in an external system. A staff user would be required to use the VistA system, or a VistA connecting system to remove the file and could then use EPSI web-based application or a system such as VistA Imaging capture to upload the correct document. EPSI is not a system of record.

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that

even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The individual is not required to correct inaccurate document uploads. The individual would contact their VA healthcare team and the healthcare team would follow national document indexing guidelines (published by HIMS or IVC) in order to correct the mistake.

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.

The EPSI web-based application does not provide individuals with the ability to determine if their documents are contained in the system. The EPSI web-based application is simply a throughput to the patient's electronic health record (EHR). Documents unindexed do not have a patient yet identified and no way to know if that individuals' documents are contained there, and documents indexed have been uploaded to the patient's records and can be accessed through MyHealtheVet or their primary healthcare team.

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: There is a risk that a Veteran could accidentally provide incorrect information to the VA, and that data could make its way into the EPSI web-based application system via the VistA passthrough.

Mitigation: Veteran who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or who want to review the contents of such a record, should submit a written request or apply in person to the VA health care facility (or directly to the VHA) where care was rendered. 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.

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.

Users are granted role-based access by their local system administrators. However, a user needs to have SSOi and VistA authorized access (determined via headers delivered by SSOi at login) to be eligible for access to the system at all. If a user has access to both SSOi and VistA, it is up to the site to determine who is granted the indexer (write) vs the QA (quality assurance) (read) role. These roles can be revoked or adjusted as required by the local administrators at any time.

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?

Initial site administrators are determined by VA Form 9957 access requests submitted to VistA Integration Adapter (VIA) support ticket to the EPSI web-based application program. No users from other agencies may have access to the system.

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

The system has 4 roles. 1. Administrator – responsible for setting users at different permission levels, updating the site specific mapping documentation. 2. Indexer – responsible for uploading the external documents into the UI and matching the patient information contained with the end indexing. 3. Nurse – Indexers can mark information for further review and make that information available to authenticated nurses for further confirmation, review and processing. 4. QA – responsible for validating the accuracy of indexing completed in the system.

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.

A.). The VA Handbook 6500.6 establishes in detail the procedures, roles and responsibilities, and contract language that governs contractor access to VA systems. These guidelines are followed in granting REFDOC access to any contractor. Applicable procedures from VA Handbook 6500.6 on contractor security requirements: Information generated by a contractor or subcontractor as part of the contractor/subcontractor's normal business operations, such as health record information created in the course of providing treatment or health care services to VA's Veterans is subject to review to determine if the information is owned by VA and subject to VA security policy. VA sensitive information that has been properly disclosed by VA to the contractor is not subject to the VAAR security clause. If the information is not owned by VA, the requirements outlined in this Handbook do not apply and the VAAR security clause should not be added to the contract. The CO, the PO, and if required, Regional Counsel can be consulted. VA OIG counsel will conduct the review for the OIG generated contracts. B.) VA requires that facilities and program offices ensure that contractors, subcontractors, and third-party servicers or associates, or on behalf of any of these entities, regardless of format or whether the VA information resides on a VA system or contractor/subcontractor's electronic information system(s) operating for or on VA's behalf, employ adequate security controls as appropriate in accordance with VA directives and handbooks, regulations, guidance, and established service level agreements. C.). Information security requirements must be considered in all phases or stages of VA's procurement process. The applicable Program Manager, Information System Owner, and Information Owner are responsible for ensuring that the solicitation document includes the appropriate information security and privacy requirements. The information security requirements must be sufficiently detailed to enable service providers to understand what is required. A general statement that the service provider must agree to comply with applicable requirements is not acceptable. See Appendix C for a catalog of security and privacy language statements that have been developed, reviewed, and approved and can be used in contracts, as appropriate. This language summarizes for the contractors the most important Federal and VA policy issues that need to be addressed, as appropriate, in contracts to ensure adequate security and privacy controls are included in the contract vehicle. Additional security or privacy language can be added, as required. Program managers, project designers, and acquisition professionals must take security requirements, measures, and controls into account when designing and making agency acquisitions; appropriate security controls drive requirements, specifications, deliverables, and costs. Acquisition staffs need to consult information security officials to determine what level of security and which security controls may be required in this process. VA Handbook 6500, Information Security Program, provides the

security requirements and policy for VA.D.) The applicable VA Program Manager, Information System Owner, Information Owner, the CO, PO, ISO, and the Contracting Officer's Technical Representative (COTR) are responsible for ensuring that VA information system security and privacy requirements, as appropriate, are implemented and complied with per the requirements detailed in the contract. Compliance and Records Management Officers should also be contacted, as appropriate, to ensure the requirements and language they require are included in the contract. E.) VA requires that all facilities and program offices monitor information security control compliance of their respective contracts and acquisitions by doing the following: (1) Adhere to the security and privacy contract language as outlined in the contracts.(2) Ensure that COs work with their COTR, ISO, and PO and other applicable staff to complete Appendix A for all service acquisitions and contracts. This appendix assists in determining the security requirements for VA acquisitions and contracts during the planning phase of the acquisition process. The checklist must be included as part of the overall contract file by the CO for new service acquisitions and contracts and a copy must be maintained in the applicable contracts file and accessible to the COTR, ISO, and PO. (3) Ensure that contracting officials include VA's approved security clause, Appendix B, into any applicable contracts, if required as indicated by completing Appendix A. NOTE: The security clause in Appendix B is currently undergoing official VA rulemaking by the Office of Acquisitions and Logistics (OA&L). The final version of the clause may be revised after it is presented to the public for review via the Federal Register. (4) Ensure that contractors, third party partners, and servicers implement the VA security and privacy requirements, as defined in the contract. These requirements can also be added to the contract Statement of Work (SOW). The requirements apply to applicable contracts in which VA sensitive information is stored, generated, transmitted, or exchanged by VA, a contractor, subcontractor or a third-party, or on behalf of any of these entities regardless of format or whether it resides on a VA system or contractor or subcontractor's electronic information system(s) operating for or on the VA's behalf. (5) Ensure that contractor systems that have negotiated with VA to store, generate, transmit, or exchange VA sensitive information in a contractor developed and maintained system are certified and accredited (authorized), and registered and monitored in VA's Security Management and Reporting Tool (SMART) database that monitors FISMA compliance. The Program Manager and/or the ISO are responsible for contacting the Information Protection and Risk Management's (IPRM) Certification Program Office (CPO) within OI&T to register the system or to answer questions regarding the authorization of systems(6) Ensure that Certification and Accreditation (Authorization) (C&A), is accomplished in compliance with VA policy (per the results of the completed checklist provided in Appendix A) and VA Handbook 6500.3, Certification and Accreditation of VA Information Systems. The OI&T CPO within the Office of Cyber Security (OCS) must be contacted regarding procedures for C&A (Authorization) of contractor managed systems. (7) Ensure that the Program Manager, the COTR and the CO, with the assistance of the ISO, monitor compliance with the contract or agreement security requirements throughout the life of the contract. For IT systems, this includes ensuring that annual self-assessments are conducted by the contractor with appropriate Plan of Actions and Milestones (POA&M) initiated and completed. (8) Ensure that service providers and contractors who have negotiated agreements with VA that involve VA sensitive information, but do not maintain systems that require C&A, complete a Contractor Security Control Assessment (CSCA) within 30 days of contract approval and annually on the due date of the contract renewal. The ISO/COTR or CO can also request that a CSCA be completed by the contractor anytime there are potential security issues identified or suspected by VA or to ensure that applicable security controls are being implemented. The completion of the CSCA by the contractor is the responsibility of the COTR. The CSCA template is maintained on the IPRM portal under the C&A Section. The COTR can contact the ISO to obtain a copy of the CSCA from the portal or to seek assistance in the completion of the assessment. The completed CSCA must be

provided and reviewed by the ISO and by the CPO to ensure that adequate security is being addressed by contractors in situations where the C&A of a system is not applicable. A copy of the CSCA is uploaded by the ISO and maintained in the document section of the SMART database. (9) Ensure that contractors and third-party servicers accessing VA information sign the Contractor Rules of Behavior, Appendix D. The VA National Rules of Behavior do not need to be signed if the VA Contractor Rules of Behavior" are signed. (10) Ensure that contractors and third-party service positions receive the proper risk level designation based upon the review of the Position Designation System and Automated Tool (PDAT) established by the Operations, Security, and Preparedness Office (007). Background investigations of all contractors must adhere to the results of the PDAT per VA Directive and Handbook 0710, Personnel Suitability and Security Program.(11) Ensure that contractors take the required security and privacy training as outlined in Appendix C. (12) Ensure that all IT procurements, including contracts, are submitted through the IT Acquisition Request System (ITARS), VA's acquisition approval system for review and approval as required by the VA CIO. (13) Ensure that language is included in appropriate contracts to ensure new acquisitions include Federal Desktop Core Configuration (FDCC) settings and products of information technology providers operate effectively using them. Link to VA Handbook 6500.6: Contractors must take approved VA security training and sign the VA Rules of Behavior document Located in VA Handbook 6500.6 Appendix C.

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.

Due to EPSI being a passthrough for information to VistA, and the EPSI web-based application validating that a user is currently authorized VistA access (via the VistAID headers returned by the SSOi login). Any training requirements that are placed on VistA for access would be the same requirements required for EPSI. The EPSI web-based application is unusable without VistA access. All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually via the VA Talent Management System.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Not Yet Approved
2. *The System Security Plan Status Date:* February10, 2023
3. *The Authorization Status:* ATO
4. *The Authorization Date:* May 18, 2023
5. *The Authorization Termination Date:* May 17, 2024
6. *The Risk Review Completion Date:* 05/16/2023

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

ATO received.

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 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 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.*

Please provide response here

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.

Please provide response here

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.

Please provide response here

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).

Please provide response here

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 provided in this Privacy Impact Assessment is true and accurate.

MICHAEL HARTMANN

Digitally signed by MICHAEL HARTMANN
Date: 2023.09.27 11:32:06 -06'00'

Privacy Officer, Michael Hartmann

MERLE KELLEY

Digitally signed by MERLE KELLEY
Date: 2023.09.29 10:22:57 -05'00'

Information Systems Security Officer, Merle Kelley

CHRISTOPHER BROWN

Digitally signed by CHRISTOPHER BROWN
Date: 2023.09.27 16:17:20 -05'00'

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).

- Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES
- 23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
- 24VA10A7, Patient Medical Records - VA (10/2/2020)
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) - VA (12-23-2020)
- 114VA10, The Revenue Program-Billing and Collections Records - VA (1/25/2021)

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