Privacy Impact Assessment for the VA IT System called:

Enterprise Precision Scanning and Indexing (EPSI)
Integrated Veteran Care
Veterans Health Administration

Date PIA submitted for review:

May 11, 2022

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Michael Hartmann</td>
<td><a href="mailto:Michael.Hartmann@va.gov">Michael.Hartmann@va.gov</a></td>
<td>303-780-4753</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Bobbi Begay</td>
<td><a href="mailto:Bobbi.Begay@va.gov">Bobbi.Begay@va.gov</a></td>
<td>720-788-4518</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Chris Brown</td>
<td><a href="mailto:Christopher.Brown1@va.gov">Christopher.Brown1@va.gov</a></td>
<td>202-270-1432</td>
</tr>
</tbody>
</table>
Abstract

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

The Enterprise Precision Scanning and Indexing (EPSI) web-based application will be used to streamline Veteran’s Affairs (VA) acceptance and temporary storage of Portable Document Format (PDF) records received from the community care 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:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes
- Whether the completion of this PIA could potentially result in technology changes
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

Enterprise Precision Scanning and Indexing (EPSI) is sponsored by Enterprise Program Management Office, Telehealth and Community Care product line in Office of Community Care, Veterans Health Administration. 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.

EPSI will not permanently store any patient information, it is primarily a workflow application that provides a means for VHA staff to upload files to the patient record in VistA Imaging. The staff at a
VA medical center (VAMC) have already received the electronic information files, typically faxed PDF electronic documents, from a community care provider. These PDFs are uploaded to the EPSI web-based application where they can be reviewed and indexed. Once they are assigned to a patient’s consult in the system, they are transferred to patients record in VistA Imaging. This information is used to further enhance the patient’s medical record.

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.

EPSI will have connections to VistA Imaging Exchange (VIX), Centralized VistA Imaging Exchange (CVIX), the Corporate Data Warehouse (CDW), SSOi, and will be accessible to users via a web browser only on the VA network.

The completion of this PIA will not result in circumstances that require changes to business processes and will not potentially result in technology changes.

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

Authority to collect is stated in SORNs:
23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020) (Cloud Authorized)
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) (Cloud Authorized)

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 Account Information
- Health Insurance Beneficiary Numbers
- Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Gender
- Integration Control Number (ICN)
- Military History/Service Connection
- Next of Kin
- Other Unique Identifying Information (list below)

PII Mapping of Components

EPSI web-application consists of two 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.

PII Mapped to Components

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

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>epsi_db</td>
<td>Yes</td>
<td>Yes</td>
<td>Integration Control Number, Name, Date of Birth, Faxed document content in PDF format, which may include: Social Security Number, Medical Health Information, Medical Records</td>
<td>Used to identify the correct patient and record for document uploading and auditing.</td>
<td>Stored in encrypted Amazon Rational Database Service (RDS) Aurora and data is destroyed by overwriting with null values after 30 days.</td>
</tr>
<tr>
<td>CDW</td>
<td>Yes</td>
<td>No</td>
<td>Integration Control Number, Consult Uniform Resource Name</td>
<td>Used to identify the correct consult to link consult related documents to</td>
<td>Data in transit is encrypted using FIPS-140-2 encryption (certificate#: 1747 – OpenSSL encryption, 3139). Data is not stored in the EPSI database and is overwritten with null values once it is no longer relevant to the indexer or that indexing process.</td>
</tr>
</tbody>
</table>

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

*List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?*
Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The 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.

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.
Information 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).

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract. This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Information 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.

1.5 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

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

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

The EPSI web-based application only collects data that is absolutely required to index and upload the document. No data that does not directly support the application is collected or stored.

All data that is collected and stored by the EPSI web-based application is absolutely necessary in order to upload documents to the patients Electronic Health Record (EHR).

The EPSI web-based application requires staff users to input patient names, select consults, note titles, and verify or input long descriptions. Any input that is not directly collected from the staff user is pulled from data sources / Application Program Interfaces (APIs) based on the staff user’s input, in order to avoid human error such as consult numbers and patient ICNs.

The EPSI web-based application does not store PII for patient search. In order to ensure the PII is accurate and current the EPSI web-based application queries the VIX service for the most current data each time a patient search is made. The EPSI web-based application then attaches the patient ICN to the file to be uploaded.

**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.
The following policies and procedures in the VA ensure that any PII collected and maintained by the VA is accurate, relevant, timely, and complete for the purpose for which it is to be used:

Requires a Veteran or an authorized representative to validate PII during the collection process. When required, request Veteran or an authorized representative to revalidate that PII collected is still accurate.
Confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information.
Collects PII directly from the individual to the greatest extent practicable.
Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems.
Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

**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 Integrated Veteran Care (IVC) and Health Information Management (HIM) review.

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

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

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

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

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?

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

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

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

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.

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

How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

**Principle of Use Limitation:** Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

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). Authorization for the access is requested by the users through the SSOi provision process (integration of this piece is currently in progress).

**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

Uploaded documents are retained in the system until they have been uploaded to a patient record or manually removed from the system.

**3.2 How long is information retained?**

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

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

This question is related to privacy control DM-2, Data Retention and Disposal.
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)? If so please indicate the name of the records retention schedule.

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

This question is related to privacy control DM-2, Data Retention and Disposal.

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.

EPSI follows VHA Records Control Schedule (RCS 10-1) https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

6000.2 Electronic Health Record (EHR).

RCS Item Number 6000.2. 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 of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?

This question is related to privacy control DM-2, Data Retention and Disposal

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

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.

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.*
<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>VistA Imaging Exchange (VIX)</td>
<td>Patient Integration Control Number, Consult Uniform Resource Name are retrieved from and then returned to VIX in order to correctly identify the patient’s record. The document is sent along with the API call back to VIX to be stored in the patients record</td>
<td>Integration Control Number, Name, Date of Birth, Social Security Number, Consult Uniform Resource Name, Progress note document (PDF healthcare document to be uploaded)</td>
<td>Data in transit is encrypted using FIPS-140-2 encryption (certificate #: 1747 - OpenSSL encryption, 3139) to transmit data securely</td>
</tr>
<tr>
<td>Central VistA Imaging Exchange (CVIX)</td>
<td>CVIX provides a centralized interface for VIX data retrieval and VIX is the specific call back. Patient Integration Control Number, Consult Uniform Resource Name are retrieved from and then returned to CVIX in order to correctly identify the patient’s record. The document is sent along with the API call back to VIX to be stored in the patients record</td>
<td>Consults &lt;URN, DATE, NUMBER OF NOTES, PROCEDURE, SERVICE, STATUS&gt; Patients &lt;NAME, DOB, ICN, SENSITIVITY, SSN&gt; Notes &lt;AUTHOR NAME, AUTHOR DUZ, DATE, HOSPITAL LOCATION, IMAGE COUNT, PATIENT NAME, PATIENT TIU NOTE URN, SIGNATURE STATUS, SITE VIX URL, TITLE&gt;</td>
<td>Data in transit is encrypted using FIPS-140-2 encryption (certificate #: 1747 - OpenSSL encryption, 3139) to transmit data securely</td>
</tr>
</tbody>
</table>
4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. This question is related to privacy control UL-1, Internal Use.

**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 PI/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.

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veterans Health Administration (VHA) Identity and Access Management (IAM)</td>
<td>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.</td>
<td>User &lt;ad domain, ad email, ad sam account name, vista id’s, vista site’s, first name, last name, sec id&gt;; User &lt;secid, username, roles&gt;; Authentication token for VistA</td>
<td>HTTPS Data in transit is encrypted using FIPS-140-2 encryption (certificate#: 1747 – OpenSSL encryption, 3139) to transmit data securely</td>
</tr>
</tbody>
</table>
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

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

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 notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

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

This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.
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.

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) (Cloud Authorized)
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) (Cloud Authorized)

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.
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

**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**: Privacy practice notices are provided to the Veteran at the time of service. This is 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?**

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

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

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

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

An individual can, at any time, request their health records through existing My HealtheVet 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.

**7.2 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.

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

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?

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

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

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.

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.*

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 My HealtheVet or their primary healthcare team.

**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**: A 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 healthcare 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?**

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

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?
Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

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

Users request initial access to the EPSI web-based application by going to https://yourit.va.gov selecting the EPSI web-based application and inputting the site and roles they would like access to. The request is then routed to the selected site’s administrators for approval. Once approved, a site administrator can change the roles a user has access to within the EPSI web-based application. The same process is followed for administrators however an elevated approval group is utilized for administrators that includes the business PM and existing site administrators. This model enables initial site administrators to request access to the site which can be approved by the product office.

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.

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.

De-provisioning is also handled through this process and users removed from the VA system are automatically removed from the EPSI web-based application via the SSOi provisioning system.

A user must have requested access to the EPSI web-based application and the desired site’s VistA in order to use the EPSI web-based application, if either access is not obtained a user will receive an error when attempting to access the EPSI web-based application.

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.
The system makes no differentiation between VA contractors or VA employees. If a user has access to SSOi and VistA at the site, and has been granted roles by the site administrator, the user is then authorized access to the system.

Since a VA Network connection is required to access the site, the EPSI web-based application possess the same requirement for access as the VA Network, or any VistA remote access connection.

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.

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

If Yes, provide:

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

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

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


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 5177. 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).

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.

The EPSI web-based application system is hosted by the VA Enterprise Cloud (VAEC) 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)

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

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.

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.
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).
# Section 10. References

## Summary of Privacy Controls by Family

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

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

Michael D Hartmann 1612370

Privacy Officer, Michael Hartmann

BOBBI DEE BEGAY

Information Systems Security Officer, Bobbi Begay

Christopher Brown 101386

Information Systems Owner, Chris 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):

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020) (Cloud Authorized)
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) (Cloud Authorized)


Department of Veterans Affairs
Veterans Health Administration
NOTICE OF PRIVACY PRACTICES
Effective Date September 30, 2019

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED OR DISCLOSED AND HOW YOU CAN GET ACCESS TO YOUR INFORMATION.

PLEASE REVIEW IT CAREFULLY

The Department of Veterans Affairs (VA), Veterans Health Administration (VHA) is required by law to maintain the privacy of your protected health information and to provide you with notice of its legal duties and privacy practices. VHA may use or disclose your health information without your permission for treatment, payment and health care operations, and when otherwise required or permitted by law. This Notice outlines the ways in which VHA may use and disclose your health information without your permission as required or permitted by law. For VHA to use or disclose your information for any other purposes, we are required to get your permission in the form of a signed, written authorization. VHA is required to maintain the privacy of your health information as outlined in this Notice and its privacy policies. Please read through this Notice carefully to understand your privacy rights and VHA's obligations.

YOUR PRIVACY RIGHTS

Right to Review and Obtain a Copy of Health Information. You have the right to review and obtain a copy of your health information in our records. You must submit a written request to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. The VHA Privacy Office at Central Office in Washington, D.C. does not maintain VHA health records, nor past military service health records. For a copy of your military service health records, please contact
the National Personnel Records Center at (314) 801-0800. The Web site is

**Right to Request Amendment of Health Information.** You have the right to request an
amendment (correction) to your health information in our records if you believe it is incomplete,
inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the
information that you want corrected, and provide a reason to support your request for amendment. All
amendment requests should be submitted to the facility Privacy Officer at the VHA health care
facility that maintains your information or health records.

*If your request for amendment is denied, you will be notified of this decision in writing and
given information about your right to appeal the decision. In response, you may do any of the
following:*

- File an appeal.
- File a "Statement of Disagreement" which will be included in your health record
- Ask that your initial request for amendment accompany all future disclosures of the disputed
  health information

**Right to Request Receipt of Communications in a Confidential Manner.** You have the right to
request that we provide your health information to you by alternative means or at an alternative
location. We will accommodate reasonable requests, as determined by VA/VHA policy, from you to
receive communications containing your health information:

- At a mailing address (e.g., confidential communications address) other
  than your permanent address.
- In person, under certain circumstances.

**Right to Request Restriction.** You may request that we not use or disclose all or part of
your health information to carry out treatment, payment or health care operations, or that
we not use or disclose all or part of your health information with individuals such as your
relatives or friends involved in your care, including use or disclosure for a particular
purpose or to a particular person.

Please be aware, that because VHA, and other health care organizations are "covered entities"
under the law, VHA is not required to agree to such restriction, except in the case of a
disclosure restricted under 45 CFR § 164.522(a)(1)(vi). This provision applies only if the
disclosure of your health information is to a health plan for the purpose of payment or health
care operations and your health information pertains solely to a health care service or visit
which you paid out of pocket in full. However, VHA is not legally able to accept an out-of-
pocket payment from a Veteran for the full cost of a health care service or visit. We are only
able to accept payment from a Veteran for co-payments. Therefore, this provision does not
apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of
your health information to a health plan for the purpose of receiving payment for health care
services VA provided to you.

To request a restriction, you must submit a written request that identifies the information you
want restricted, when you want it to be restricted, and the extent of the restrictions. All requests
to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA
health care facility that provided or paid for your care. If we agree to your request, we will
honor the restriction until you revoke it unless the information covered by the restriction is
needed to provide you with emergency treatment or the restriction is terminated by VHA upon notification to you.

**NOTE:** We are not able to honor requests to remove all or part of your health information from the electronic database of health information that is shared between VHA and DoD, or to restrict access to your health information by DoD providers with whom you have a treatment relationship.

**Right to Receive an Accounting of Disclosures.** You have the right to know and request a copy of what disclosures of your health information have been made to you and to other individuals outside of VHA. To exercise this right, you must submit a written request to the facility Privacy Officer at the VHA health care facility that provides your care.

**Right to a Printed Copy of the Privacy Notice.** You have the right to obtain an additional paper copy of this Notice from your VHA health care facility. You can obtain this Notice from the facility Privacy Officer at your local VHA health care facility. You may also obtain a copy of this Notice at the following website: [http://www.va.gov/vhapublications](http://www.va.gov/vhapublications).

**Notification of a Breach of your Health Information.** If a breach of any of your protected health information occurs, we will notify you and provide instruction for further actions you may take, if any.

**Complaints.** If you are concerned that your privacy rights have been violated, you may file a complaint with:

- VA via the Internet through "Contact the VA" at [http://www.va.gov](http://www.va.gov) or by dialing 1-800-983-0936 or by writing the VHA Privacy Office (10A7) at 810 Vermont Avenue NW, Washington, DC 20420.
- Complaints do not have to be in writing, though it is recommended. An individual filing a complaint will not face retaliation by any VA/VHA organization or VA/VHA employee.

**When We May Use or Disclose Your Health Information without Your Authorization**

**Treatment.** We may use and disclose your health information without your authorization for treatment or to provide health care services. This includes using and disclosing your information for:

- Emergency and routine health care or services, limited to labs and x-rays, clinic visits, inpatient admissions
- Contacting you to provide appointment reminders about treatment alternatives
- Seeking placement in community living centers or skilled nursing homes
- Providing or obtaining home-based services or hospice services
- Filling and submitting prescriptions but not for medications, supplies, and equipment
- Coordination of care, including care from non-VHA providers
- Communicating with non-VHA providers regarding your care through health information exchanges
- Coordination of care with DoD, including electronic information exchange

**NOTE:** If you are an active-duty service member, Reservist or National Guard member, your health information can be used or disclosed without your authorization in certain circumstances related to your military service or participation in military campaigns.
information is available to DoD providers with whom you have a treatment relationship. Your protected health information is on an electronic database that is shared between VHA and DoD. VHA does not have the ability to restrict DoD's access to your information in this database, even if you ask us to do so.

**Examples:**

1) A Veteran sees a VHA doctor who prescribes medication based on the Veteran's health information. The VHA pharmacy uses this information to fill the prescription.
2) A Veteran is taken to a community hospital emergency room. Upon request from the emergency room, VHA discloses health information to the non-VHA hospital staff that needs the information to treat this Veteran.
3) A National Guard member seeks mental health care from VHA. VHA discloses this information to DoD by entering the information into a database that may be accessed by DoD providers at some future date.
4) A Veteran is seen by his community health care provider, who wants to review the Veteran's last blood work results from his VHA Primary Care visit for comparison. The community health care provider uses a local health information exchange to request and receive the results from VHA to better care for the Veteran.

**Payment.** We may use and disclose your health information without your authorization for payment purposes or to receive reimbursement for care provided. This includes using and disclosing your information for:

- Determining eligibility for health care services
- Paying for non-VHA care and services, including but not limited to, CHAMPVA, Choice and fee basis
- Coordinating benefits with other insurance payers
- Finding or verifying coverage under a health insurance plan or policy
- Pre-certifying insurance benefits
- Billing and collecting for health care services provided by VHA
- Reporting to consumer reporting agencies regarding delinquent debt owed to VHA

**Examples:**

1) A Veteran is seeking care at a VHA health care facility. VA uses the Veteran's health information to determine eligibility for health care services.
2) The VHA health care facility discloses a Veteran's health information to a private health insurance company to seek and receive payment for the care and services provided to the Veteran.
3) A Veteran owes VA $5000 in copayments for Non-Service Connected care over two years. The Veteran has not responded to reasonable administrative efforts to collect the debt. VA releases information concerning the debt, including the Veteran's name and address, to a consumer reporting agency for the purpose of making the information available for third-party decisions regarding such things as the Veteran's credit, insurance, housing, banking services, utilities.

**Health Care Operations.** We may use or disclose your health information without your authorization to support the activities related to health care. This includes using and disclosing your information for:

- Improving quality of care or services
- Conducting Veteran and beneficiary satisfaction surveys
- Reviewing competence or qualifications of health care professionals
- Providing information about treatment alternatives or other health-related benefits and services
- Conducting health care training programs
- Managing, budgeting and planning activities and reports
- Improving health care processes, reducing health care costs and assessing organizational performance
- Developing, maintaining and supporting computer systems
- Addressing patient complaints
- Legal services
- Conducting accreditation activities
- Certifying, licensing, or credentialing of health care professionals
- Conducting audits and compliance programs, including fraud, waste and abuse
Performing process reviews and root cause analyses

Examples:

1) Medical Service, within a VHA health care facility, uses the health information of diabetic Veterans as part of a quality-of-care review process to determine if the care was provided in accordance with the established clinical practices.
2) A VHA health care facility discloses a Veteran's health information to the Department of Justice (DOJ) attorneys assigned to VA for defense of VHA in litigation.
3) The VHA health care facility Utilization Review Committee reviews care data, patient demographics, and diagnosis to determine that the appropriate length of stay is provided per Utilization Review Standards.

Eligibility and Enrollment for Federal Benefits. We may use or disclose your health information without your authorization to other programs within VA or other Federal agencies, such as the Veterans Benefits Administration, Internal Revenue Service, or Social Security Administration, to determine your eligibility for Federal benefits.

Abuse Reporting. We may use or disclose your health information without your authorization to report suspected child abuse, including child pornography; elder abuse or neglect; or domestic violence to appropriate Federal, State, local, or tribal authorities. This reporting is for the health and safety of the suspected victim.

Serious and Imminent Threat to Health and Safety. We may use or disclose your health information without your authorization when necessary to prevent or lessen a serious and imminent threat to the health and safety of the public, yourself, or another person. Any disclosure would only be to someone able to help prevent or lessen the harm, such as a law enforcement agency or the person threatened. You will be notified in writing if any such disclosure has been made by a VHA health care facility.

Public Health Activities. We may disclose your health information without your authorization to public health and regulatory authorities, including the Food and Drug Administration (FDA) and Centers for Disease Control (CDC), for public health activities. This includes disclosing your information for:

- Controlling and preventing Disease, injury, or disability
- Reporting communicable diseases, such as hepatitis, tuberculosis, sexually transmitted diseases & HIV
- Reporting adverse events and product defects or problems
- Enabling product recalls, repairs or replacements
- Tracking FDA-regulated products
- Reporting certain information to identify or

Judicial or Administrative Proceedings. We may disclose your health information without your authorization for judicial or administrative proceedings, such as when we receive an order of a court, such as a subpoena signed by a judge, or administrative tribunal, requiring the disclosure.

Law Enforcement. We may disclose your health information without your authorization to law enforcement agencies for law enforcement purposes when applicable legal requirements are met. This includes disclosing your information for:

- Identifying or apprehending an individual who has admitted to participating in a violent crime
- Reporting a death where there is a suspicion that
- Routine reporting to law enforcement agencies, such as gunshot wounds
- Providing certain information to identify or
death has occurred as a result of a crime
• Reporting Fugitive Felons
• Investigating a specific criminal act

Health Care Oversight. We may disclose your health information without your authorization to a governmental health care oversight agency (e.g., Inspector General; House Veterans Affairs Committee) for activities authorized by law, such as audits, investigations, and inspections. Health care oversight agencies include government agencies that oversee the health care system, government benefit programs, other government regulatory programs, and agencies that enforce civil rights laws.

Cadaveric Organ, Eye, or Tissue Donation. When you are an organ donor and death is imminent, we may use or disclose your relevant health information without your authorization to an Organ Procurement Organization (OPO), or other entity designated by the OPO, for determining suitability of your organs or tissues for organ donation. If you have not specified your donation preferences and can no longer do so, your family may make the determination regarding organ donation on your behalf.

Coroner or Funeral Services. Upon your death, we may disclose your health information to a funeral director for burial purposes, as authorized by law. We may also disclose your health information to a coroner or medical examiner for identification purposes, determining cause of death, or performing other duties authorized by law.

Services. We may provide your health information without your authorization to individuals, companies and others who need to see your information to perform a function or service for or on behalf of VHA. An appropriately executed contractual document, if applicable, and business associate agreement must be in place to ensure the contractor will appropriately secure and protect your information.

National Security Matters. We may use and disclose your health information without your authorization to authorized Federal officials for conducting national security and intelligence activities. These activities may include protective services for the President and others.

Workers' Compensation. We may use or disclose your health information without your authorization to comply with workers' compensation laws and other similar programs.

Correctional Facilities. We may disclose your health information without your authorization to a correctional facility if you are an inmate and disclosure is necessary to provide you with health care; to protect the health and safety of you or others; or for the safety of the correctional facility.

Required by Law. We may use or disclose your health information without your authorization for other purposes to the extent required or mandated by Federal law (e.g., to comply with the Americans with Disabilities Act; to comply with the Freedom of Information Act (FOIA); to comply with a Health Insurance Portability and Accountability Act (HIPAA) privacy or security rule complaint investigation or review by the Department of Health and Human Services).

Activities Related to Research. Before we may use health information for research, all research projects must go through a special VHA approval process. This process requires an Institutional Review Board (IRB) to evaluate the project and its use of health information based on, among other things, the level of risk to you and to your privacy. For many research projects, including
any in which you are physically examined or provided care as part of the research, you will be asked to sign a consent form to participate in the project and a separate authorization form for use and possibly disclosure of your information. However, there are times when we may use your health information without an authorization, such as, when:

- A researcher is preparing a plan for a research project. For example, a researcher needs to examine patient medical records to identify patients with specific medical needs. The researcher must agree to use this information only to prepare a plan for a research study; the researcher may not use it to contact you or actually conduct the study. The researcher also must agree not to remove that information from the VHA health care facility. These activities are considered preparatory to research.
- The IRB approves a waiver of authorization to use or disclose health information for the research because privacy and confidentiality risks are minimal and other regulatory criteria are satisfied.
- A Limited Data Set containing only indirectly identifiable health information (such as dates, unique characteristics, unique numbers or zip codes) is used or disclosed, with a data use agreement (DUA) in place.

**Military Activities.** We may use or disclose your health information without your authorization if you are a member of the Armed Forces, for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, when applicable legal requirements are met. Members of the Armed Forces include Active-Duty Service members and in some cases Reservist and National Guard members.

*Example:* Your Base Commander requests your health information to determine your fitness for duty or deployment.

**Academic Affiliates.** We may use or disclose your health information without your authorization to support our education and training program for students and residents to enhance the quality of care provided to you.

**State Prescription Drug Monitoring Program (SPDMP).** We may use or disclose your health information without your authorization to a SPDMP in an effort to promote the sharing of prescription information to ensure safe medical care.

**General Information Disclosures.** We may disclose general information about you without your authorization to your family and friends. These disclosures will be made only as necessary and on a need-to-know basis consistent with good medical and ethical practices, unless otherwise directed by you or your personal representative. General information is limited to:

- Verification of identity
- Your condition described in general terms (e.g., critical, stable, good, prognosis poor)
- Your location in a VHA health care facility (e.g., building, floor, or room number)

**Verbal Disclosures to Others While You Are Present.** When you are present, or otherwise available, we may disclose your health information to your next-of-kin, family or to other individuals that you identify. Your doctor may talk to your spouse about your condition while at your bedside or in the exam room. Before we make such a disclosure, we will ask you if you object or if it is acceptable for the person to remain in the room. We will not make the disclosure if you object.

**Verbal Disclosures to Others When You Are Not Present.** When you are not present, or are unavailable, VHA health care providers may discuss your health care or payment for your health care.
with your next-of-kin, family, or others with a significant relationship to you without your authorization. This will only be done if it is determined that it is in your best interests. We will limit the disclosure to information that is directly relevant to the other person's involvement with your health care or payment for your health care.

Examples of this type of disclosure may include questions or discussions concerning your in-patient medical care, home-based care, medical supplies such as a wheelchair, and filled prescriptions.

**IMPORTANT NOTE:** A copy of your medical records can be provided to family, next-of-kin, or other individuals involved in your care only if we have your signed, written authorization or if the individual is your authorized personal representative.

**Other Uses and Disclosures with Your Authorization.** We may use or disclose your health information for any purpose you specify in a signed, written authorization you provide us. Your signed, written authorization is always required to disclose your psychotherapy notes, if they exist. If we were to use or disclose your health information for marketing purposes, we would require your signed written authorization. In all other cases, we will not use or make a disclosure of your health information without your signed, written authorization, unless the use or disclosure falls under one of the exceptions described in this Notice. When we receive your signed, written authorization we will review the authorization to determine if it is valid, and then disclose your health information as requested by you in the authorization.

**Revocation of Authorization.** If you provide us a signed, written authorization to use or disclose your health information, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your health information unless the use or disclosure falls under one of the exceptions described in this Notice or as otherwise permitted by other laws. Please understand that we are unable to take back any uses or disclosures we have already made based on your signed, written authorization.

**When We Offer You the Opportunity to Decline the Use or Disclosure of Your Health Information**

**Patient Directories.** Unless you opt-out of the VHA medical center patient directory when being admitted to a VHA health care facility, we may list your general condition, religious affiliation and the location where you are receiving care. This information may be disclosed to people who ask for you by name. Your religious affiliation will only be disclosed to members of the clergy who ask for you by name.

**Patient Directories.** Unless you opt-out of the VHA medical center patient directory when being admitted to a VHA health care facility, we may list your general condition, religious affiliation and the location where you are receiving care. This information may be disclosed to people who ask for you by name. Your religious affiliation will only be disclosed to members of the clergy who ask for you by name.

**NOTE:** If you object to being listed in the Patient Directory, no information will be given out about you unless there is other legal authority. This means your family and friends will not be able to find what room you are in while you are in the hospital. It also means you will not be able to receive flowers or mail, including Federal benefits checks, while you are an inpatient in the hospital or nursing home. All flowers and mail will be returned to the sender.

**When We Will Not Use or Disclose Your Health Information**
**Sale of Health Information.** We will not sell your health information. Receipt by VA of a fee expressly permitted by law, such as Privacy Act copying fees or FOIA copying fees is not a "sale of health information."

**Genetic Information.** We will not use or disclose genetic information to determine your eligibility for or enrollment in VA health care benefits.

**Changes to This Notice:** We reserve the right to change this Notice. The revised privacy practices will pertain to all existing health information, as well as health information we receive in the future. Should there be any changes to this Notice we will make a copy of the revised Notice available to you within 60 days of any change. The Notice will contain the effective date on the first page.

**Contact Information:** You may the Privacy Officer at your local VHA health care facility if you have questions regarding the privacy of your health information or if you would like further explanation of this Notice. The VHA Privacy Office may be reached by mail at VHA Privacy Office, Office of Health Informatics (10A7), 810 Vermont Avenue NW, Washington, DC 20420 or by telephone at 1-877-461-5038 (toll free).