Privacy Impact Assessment for the VA IT System called:

Patient Advocate Tracking System Replacement (PATS-R)

BAM CRM High Assessing (#692)

Veterans Health Administration (VHA)

Veteran Experience Services (VES)

Date PIA submitted for review:

January 17, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	Thomas Orler	Thomas.Orler@va.gov	708-938-1247
Information System Owner	Stefano Masi	Stefano.Masi@va.gov	806-681-9927

Abstract

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

The PATS-R application captures Interactions between Veterans or their beneficiaries or their representatives and Patient Advocates from the Office of Patient Advocacy (OPA) through multiple channels. Patient Advocates can also leverage real-time Veteran feedback for effective service recovery. The feedback that Patient Advocates receive and manage is entered into PATS-R through multiple channels (both internal and external to the VA) such as in-person visits, phone calls or voicemails, emails, letters, and other VA systems. Regardless of channel, the Patient Advocate can open, route, track, and close Interactions. The Ask VA (AVA) application is built as a sub-system within PATS-R.

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.*

The Patient Advocate Tracking System Replacement (PATS-R) application falls under the Office of Information Technology (OI&T) Development, Security, and Operations (DevSecOps) Product Engineering (PE), Enterprise Program Management Office (EPMO), Veteran Experience Services (VES), Veteran Relationship Management (VRM) Product Line.

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

PATS-R is utilized nationwide by Office of Patient Advocacy (OPA) Patient Advocates under the auspices of the Veterans Experience Office (VEO). PATS-R serves as VA's electronic system of record for documenting the contact made by the Veteran, beneficiary, or their representatives to VA Patient Advocates and supports the Veterans Health Administration (VHA) Patient Advocacy Program's mission to resolve patient concerns with care they are receiving, and to advocate for patient and family rights.

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

PATS-R is owned by the Office of Information Technology (OI&T) Development, Security, and Operations (DevSecOps) Product Engineering (PE), Enterprise Program Management Office (EPMO), Veteran Experience Services (VES), Veteran Relationship Management (VRM) Product Line.

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.*

Since the inception of the PATS-R application in 2019 through the writing of this document Interactions for 3,472,084 unique named (i.e., excluding anonymous interactions) Patients have been entered in PATS-R. Veterans are the primary category of individuals of which PATS-R stores information.

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

The PATS-R application captures interactions between Veterans, beneficiaries, or their representatives and Patient Advocates. Patient Advocates leverage real-time Veteran feedback for effective service recovery. The feedback that Patient Advocates receive and manage is entered into PATS-R through multiple channels (both internal and external to the VA) such as in-person visits, phone calls or voicemails, emails, letters, and other systems such as the Veterans Signals (VSignals) survey tool, Whitehouse.gov "Contact Me" function, Regardless of channel, the Patient Advocate can open, route, track, and close Interactions with the goal of improving the quality of care Veterans receive.

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

PATS-R has interfaces to systems both internal and external to the VA. PATS-R includes the sub-system known as Ask VA (AVA). The PATS-R application (and AVA sub-system) displays but does not retain (unless entered into the Interaction by the Patient Advocate) data from the following VA Systems Inventory (VASI):

System Name	Alias	VASI
Master Patient Index (MPI)	N/A	#1406
VHA Enrollment System (VES)	Enrollment Application System (EAS)	#1231
Health Data Repository (HDR)	N/A	#1311
Joint Electronic Health Record System	Cerner Millennium	#2204
Veterans Signals (VSignals)	Medallia	#2141
Community Care (CommCare)	N/A	#2033
White House VA Hotline	WHHL	#2620
Summit Data Platform (SDP)	Customer Experience Data Warehouse (CxDW)	#2266
Analytics and Business Intelligence LAN	VHA Support Service Center (VSSC)	#1769
Identity and Access Management (IAM) - Single Sign-On External (SSOe)	AccessVA	#1977

The AVA sub-system replaces functionality formerly provided by the legacy system known as the Inquiry Routing Information System (IRIS) application (VASI #1347). AVA includes back-end infrastructure built within the PATS-R Dynamics Instance, and web-portal reached via a link on the *"Contact Us"* section of va.gov (or directly at ask.va.gov). AVA officially went live on October 18, 2021; while the Legacy IRIS system was decommissioned on January 31, 2021.

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.*

PATS-R has been fielded across the United States and Territories. PATS-R training began in August of 2018 and the national rollout was fully completed in June 2019. The PATS-R application is hosted on the Microsoft – Dynamics CRM (Dynamics 365) Online (CRMOL) for Government Cloud. The latest release of Microsoft Customer Relationship Management (CRM) is Microsoft Dynamics 365 (D365); references to CRM and D365 are synonyms with the Microsoft platform on which PATS-R is built. It is a Software-as-a-Service (SaaS) offering as defined in National Institute of Standards and Technology (NIST) SP800-145. Both the primary and backup data centers are owned by Microsoft, who is the VA contracted Cloud Service Provider (CSP) at those sites with direct connections to the VA Trusted Internet Connections (TIC) from each respective location. Personally Identifiable Information (PII) is maintained consistently, and the same controls are used across all sites utilizing the PATS-R application.

3. Legal Authority and SORN

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

The Cloud Service Provider (CSP) FedRAMP associated with PATS-R is: "Microsoft – Dynamics CRM Online for Government (CRMOL)". The Microsoft Azure Government Contract establishes VA ownership rights of all data including PII. The Contract Number is: 47QTCA22D003G; Task Order: 36C10B22F0089.

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?*

The PATS-R application is in active development and has valid System of Records Notice (SORN). PATS-R's development will not require the existing SORNs to be amended or revised. PATS-R uses cloud technology and existing SORN does cover cloud usage and storage. PATS-R's SORN is as follows: 100VA10H / 86 FR 6988; "Patient Advocate Tracking System Replacement (PATS-R)—VA" (Monday, January 25, 2021). Authority for maintenance of the system is Title 38, United States Code, Chapter 73, section 7301(b).

D. System Changes

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

No. The completion of this PIA is not expected to result in changes to business processes.

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

No. The completion of this PIA is not expected to result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Other: Location of Patient Veterans Integrated Service Network (VISN) and Facility, free text notes, VES data (Demographics, Insurance, Phone Numbers), Health Data Repository (HDR) data (Consults, Appointments, Notes, Postings, Orders). Further elaboration of the data elements that are pulled from the VistA systems and viewed, but not stored, within the PATS-R application:

- HDR VistA Consults
- HDR VistA Appointments

- HDR VistA Notes
- HDR VistA Postings
- HDR VistA Orders

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

PII Mapping of Components (Servers/Database)

PATS-R consists of **zero** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **PATS-R** 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
N/A	N/A	N/A	N/A	N/A	N/A

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 primary source of information in the PATS-R application is direct Interaction between Veteran, beneficiary or representative and OPA Patient Advocate. Patient Advocates use at least three (3) identification factors for the Veteran (last name, DoB, SSN) to search MPI. MPI returns basic personal data about a Veteran (name, address, etc.). Information obtained from MPI is used to pull data from internal VHA systems. These systems are HDR, VES, VSignals.

Source	Description
Interaction	Information from the Veteran, beneficiary or representative is recorded in CRM. Information from other systems can be confirmed by the Patient Advocate during the interaction
MPI	At Least three factors provided by the Caller (Last Name, DoB, SSN) are used to search MPI. MPI returns Veteran data which is stored in CRM as part of the Veteran’s Record. The Veteran’s Integration Control Number (ICN) is also returned by MPI and is stored by CRM.

Source	Description
VES	The ICN returned by MPI and/or is stored on the Contact is used to search VES. VES returns demographics, insurance, addresses, etc. The VES information is not stored in CRM and is only displayed to the user
HDR	The ICN returned by MPI and/or is stored on the Contact is used to search HDR. HDR returns VistA clinical data such as appointments, consults, orders, and progress notes. The HDR information is not stored in CRM and is only displayed to the user.
CommCare	An integration is available between CommCare and PATS-R so PATS-R users will not have to create dual entries for the same patient.
VSignals	This interface allow access to Medallia for Digital Comment Cards for tracking and resolution

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.

Information pulled from sources above is used to ensure Patient Advocates receive all information necessary to create the interaction. Information is verified during the interaction. PATS-R does modify data from integrated systems

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

Based on the interactions with Veterans, beneficiaries, or their representatives, Patient Advocates (or other PATS-R users) can create Cases, and Requests. Cases and Requests can contain information about the interaction recorded on the Patient Contact Object, and the Case Notes Field.

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 used in the PATS-R application is collected by Patient Advocates (or other PATS-R users) from Veterans, Veteran family members and beneficiaries, and Health Care Providers through a variety of interaction methods. PATS-R user conduct a search against MPI, which returns a Veteran's name, SSN, ICN and other details. Additional Veteran information from HDR, VES, VSignals are collected by searching those interfaces using the ICN returned by MPI. The HDR, VES, VSignals information is not stored by the system. Any request that requires information pulls it via the specified interface when that request is opened and clears the cache of data when the web browser is closed. During the interaction the PATS-R user may discover that additional actions outside of their purview is required to resolve an inquiry about a claim(s) or eligibility for benefits. As such, the PATS-R user can make an annotation in the CRM Notes field and refer the Case or Request to a supervisor or a colleague in a different VHA department, such as Debt Management, for follow-up. Although the Notes field is not intended to document PII, the CRM application does not preclude PII from being stored because it is a free form text field.

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

The information collected by PATS-R is unrelated to the Paperwork Reduction Act.

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.

Veteran / patient identity is checked for accuracy through MPI. Verification requires at least three (3) identifiers to conduct a successful MPI search. This ensures that the correct Veteran / patient is associated to a Request. Personal information from the Veteran / patient is then populated into the Request form and Veteran Record. The PATS-R user verifies with the Veteran or Beneficiary whether their information is correct. MPI is the authoritative source to validate a Veteran / patient. PATS-R user cannot directly change the information from the authoritative source (i.e., HDR, VES, VSignals within D365 (i.e., PATS-R). All integrated VHA systems perform their own data validation processes. The PATS-R application relies on the integrated systems to provide data, and only displays the data from the external systems. PATS-R is an interface application, information/data update happens in the source application per their policy and procedures.

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.

PATS-R does not use a commercial aggregator of information.

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

The PATS-R application complies with the following federal regulations and/or departmental policies and guidelines, as follows:

- Authority for maintenance of the system: Title 38, United States Code, Chapter 73, section 7301(b).
- Title 38, United States Code, Section 501-Veterans' Benefits.
- Join Commission National Patient Safety Goals- Goal 1: Improve the accuracy of patient identification.
- VHA Directive 1906- Data Quality Requirements for Healthcare Identity Management and the Master Veterans Index Functions.
- VHA Directive 2009-021 Data Entry Requirements for Administrative Data.
- VHA Directive 2006-036 Data Quality Requirements for Identity Management and the Master Patient Index Functions.
- VHA Directive 2007-037 Identity Authentication for Health Care Services.
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.
- VA Directive 6300, Records and Information Management.
- VA Handbook 6500, VA6500 AC-8: System Use Notification.
- The Privacy Act of 1974.

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: Veteran, beneficiary, or healthcare provider may provide incorrect identity information to Patient Advocate / PATS-R user.

Mitigation: Veteran / patient information is validated through MPI, as the authoritative source, before the interaction proceeds and any information is provided. Additional information gathered and provided is based on MPI-returned identifiers. The PATS-R user does not provide PII from the errant MPI search to the Veteran / patient as a means of selecting the correct Veteran or Beneficiary.

Privacy Risk: Patient Advocate / PATS-R user may enter caller-provided information erroneously.

Mitigation: Veteran / patient information is validated through MPI, as the authoritative source, before the interaction proceeds and any information is provided. Additional information gathered and provided is based on MPI returned identifiers. The Patient Advocate / PATS-R user will be aware of incorrectly entered data because the MPI search will return zero records or the MPI results will return a Veteran, Beneficiary or a Beneficiary's sponsor (Veteran) who is not the subject of the interaction. Patient Advocate / PATS-R user must validate that the correct Veteran or Beneficiary is returned from the MPI search before the CSR can proceed to review a claim and/or eligibility information. If the Veteran or Beneficiary is not validated, then the PATS-R user will not proceed with the interaction.

Privacy Risk: Data pulled by the PATS-R application contains PII. If the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft might result.

Mitigation: The PATS-R application ensures strict access to information by enforcing thorough access control and requirements for end users. Access to the application is by PIV authentication. Individual administrator user IDs and access are provided based on need. The OPA limits access rights and controls only to valid end users. There are rigorous securities monitoring controls to prevent unauthorized access and intrusion, and to protect all information. Furthermore, all end users are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. All users with access to PATS-R are responsible in assuring safeguards for PII and PHI.

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.

Interfaces with VES (Veteran demographics) and VistA (Veteran clinical information) provide dynamically constructed data feeds to help the user complete his or her work. The data is cached and displayed during the session, allowing the user to interact in a meaningful manner (the user can sort, filter, and search through datasets for specific information). When the session is complete and has ended, the cache is cleared; the bulk of the data used during the session is not stored. Only minimal, critical call information is retained by the CRM, as the system of record for phone interactions, giving management the ability to report on types of calls, first call resolution, and time to solve. The information listed below is transmitted from the VHA systems, and is pulled into the PATS-R system to verify Veteran identity and assist with telephone inquiries:

- Full Name
- Social Security Number (SSN)
- Integration Control Number (ICN)
- Date of Birth (DOB)
- Mailing Address
- Zip Code
- Phone Number(s)
- Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Previous Medical Records
- Eligibility Status
- Next of Kin (NOK) Information
- Patient Record Flags
- Name of Facility
- Appointment Information
- Prescription and Medication Information
- Consultation Information
- Lab and Diagnostic Test Information
- Progress Notes and Addenda
- Previous Encounters, Allergies, Vital Signs, Immunizations, Problem List, Postings, Chronic Illnesses
- Gender
- Military History/Service Connection

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.

The D365 (i.e., CRM) platform provides out-of-the-box reporting capabilities which can provide analysis and reports of data housed in the system. The data analysis capabilities of the Dynamics platform allow users to generate configurable reports on an ad-hoc or scheduled basis. These reports consist of a summary data that lists the number of records that meet various criteria, and basic analysis including call resolution totals and percentages. Additionally, PATS-R has implemented the push to data-lake housed in the Summit Data Platform (VASI #2266), PowerBI reporting capability, and has interfaced with the Analytics and Business Intelligence LAN (VASI #1759) to support VSSC reporting activities in the future. These reporting partners allow for analysis of data related to the interactions entered in PATS-R; there is no reporting specifically related to Veterans or beneficiaries.

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.

PATS-R does not create or make available any new or previously un-utilized clinical or benefits information about any individual. PATS-R does record interaction details between Patient Advocates / PATS-R users and customer. These details may include free-form notes and comments about the customer service issue.

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 following measures are in place to protect PATS-R data while in transit and at rest VA Network (Firewall), PIV authentication via native integration with VA Active Directory (AD), Dynamics 365 out-of- the-box encryption, and Dynamics 365 Shield Encryption. Additionally, all PATS-R users are VA employees or contractors that have been granted VA accounts contingent on completed the VA's background check and onboarding process. Users of PATS-R are specifically identified by PATS-R Site and VISN coordinators in the field and must be specifically licensed and provisioned with in the PATS-R Dynamics 365 instance and actively trained on the application's use.

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

In addition to security measures listed above the SSN fields are encrypted within PATS-R and in many places masked.

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

PII and PHI within the PATS-R application is safeguarded behind the following: VA Network (Firewall), PIV authentication via native integration with VA Active Directory (AD), Dynamics 365 out-of- the-box encryption, and Dynamics 365 Shield Encryption. Additionally, the PATS-R application is part of FedRAMP ATO certified with a National Institute of Standards and Technology (NITS) Federal Information Processing Standards (FIPS) 199 Security Classification of HIGH.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to PII and PHI is limited by the PATS-R application to only those data items deemed necessary for an application user to perform their job, as determined by their management team and their job description. Additionally, user roles are implemented to restrict user's access to only the specific information required to perform their job function. .

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

System documentation includes detailed system design and user guides that specify those areas of the system that contain PII and PHI, as well as how it is to be utilized by PATS-R users.

2.4c Does access require manager approval?

Access requests go through many layers of approvals. D365 Licenses must be approved by the OI&T Product Manager, and Provisioning is performed via the self-service User Management App by select number of users with elevated permissions in leadership roles at each site and VISN.

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

The PATS-R application implements auditing which tracks user access to the system and all data accessed. The information is mapped in the audit record by user identifier and Veteran identifier used for data access.

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. Ultimately, safeguarding PII and PHI is a core VA objective and is everyone's responsibility.

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*

The information listed below is the only information retained in the PATS-R database:

- Full Name
- SSN
- ICN
- DoB
- Mailing Address
- Zip Code
- Phone Number(s)
- Email Address
- Interaction Notes

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.*

When a D365 session is complete and has ended the cache is cleared and the bulk of data used during the session is removed. Only minimal, critical information is retained by the D365, as the system of record

Patient Advocate interactions. This information gives management the ability to report on types of calls, first call resolution, and time to solve Veteran issues. The Veteran's self-entered record is to be maintained indefinitely. National Archives and Records Administration (NARA) guidelines, as stated in the VHA Records Control Schedule (RCS) 10-1 records retention schedule, requires retention for 75 years. Whenever technically feasible, all records are retained indefinitely – in case additional follow-up actions on behalf of the individual become necessary. However, any documents the Veteran wants removed from the system will be purged from the system upon request.

VHA Records Control Schedule (RCS) 10-1 linked here.

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?

A Backup Plan and Restore Plan is developed and implemented for the cloud-hosted environment using Dynamics 365 native Backup & Restore capabilities and industry best practices.

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

Records for PATS-R are retained in accordance with Records Schedule DAA-0015-2017-0001.

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.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008). When required, this data is deleted from their file location and then permanently deleted from the Deleted Items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1 and NIST SP800-88r1 as evidenced in the FedRAMP Audit reports. The PATS-R application will follow NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process of any IT storage hardware used in the PATS-R application. The Guidelines establish three levels of data destruction: Clear, Purge, and Destroy, that can be applied to different data storage devices. An appropriate destruction method will be chosen based on the memory type (Flash Memory, Magnetic

Drives, Optical Devices, Hard Copies etc.) used for the storage. It is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws. Regarding temporary paper records, those that contain PII, and VA sensitive information, which are under the jurisdiction of VA, will be handled securely, economically, and effectively and disposed of properly. Written documentation that attests to the completion of the destruction process after the final destruction is required, which could be in the form of a letter, memo, or any format attesting to its complete destruction. This certification is not considered a valid certification of destruction if completed and submitted before the final destruction of the records. The certification should contain sufficient information to attest to the final destruction of the temporary paper records – what temporary records were destroyed, the date when they were destroyed, what destruction method was used, where they were destroyed, and who was responsible for their final destruction. Paper records are destroyed on site, destruction verification of secure shred containers is verified by the logistics department. The VHA Office of Community Care program office has a contract with Shred-it. No documents leave the facility, and system users are unable to print from a remote location.

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.

PII and PHI is not used during testing or training. Test Veterans with artificial data are used to test the application. Additionally, all training materials display example data using test Veterans. At this time, PATS-R data is not used for research. If PATS-R data is to be used for research in the future the project team will de-identify all data to minimize the risk to privacy when using PII for research.

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?*

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u> If data is maintained within the PATS-R application for a longer time-period than what is needed or required, then the risk that the information will be compromised, breached, or unintentionally released to unauthorized individuals increases.

<u>Mitigation:</u> The PATS-R application only retains information necessary for its purpose of helping Veterans, Beneficiaries, and Medical Providers with their questions regarding non-VA medical care, claims, and claims processing. When a session is complete, the cache is cleared. This production data is retained for 14 days. Information retained by the system gives management the ability to report on types of calls, first call resolution, and time to solve Veteran and Beneficiary issues. Because these data are retained indefinitely, a Backup Plan and Restore Plan is implemented for the cloud hosted environment using industry best practices. At a minimum, the plan includes the requirement to save data for the backup and recovery of information stored on the cloud storage infrastructure to meet related Service Level Agreements (SLAs), and the retention of records.

<u>Privacy Risk:</u> If Veteran data is lost via in a disaster scenario prior to being backed up, then full indefinite retention of data will not be achieved.

<u>Mitigation:</u> All primary production servers are backed up on a daily incremental and weekly full basis employing Dynamics 365 native backup & restore capabilities with the data stored in geo-redundant Microsoft Government data centers.

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***
Master Patient Index (MPI)	MPI	Information required for identity proofing and Veteran integration Control Number (ICN) for subsequent web service requests.	Encrypted electronic transmission (web service).
VHA Enrollment System (VES)	VES	Veteran demographics, contact information, enrollment information, eligibility information, service connection, sensitivity, financial assessment information, and insurance.	Encrypted electronic transmission (web service).
Health Data Repository (HDR)	HDR	Medical chart information, including, radiology reports, problems, orders, progress notes, medications, lab results, allergies, consults, appointments, and postings.	Encrypted electronic transmission (web service).
VSignals Integration	VSignals	Veteran Feedback generated from Survey, Call Center, or Social Media, VA Demographics, and Case updates.	Encrypted electronic transmission (web service).

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***
VRM Product Line	CommCare	Exchanges Veteran demographics, contact information, enrollment information, eligibility information, service connection, sensitivity, financial assessment information, and insurance.	Encrypted electronic transmission (web service).
White House Hotline Contact Center	WHHL	Veterans Inquiries, Complaints, and Compliments.	Encrypted electronic transmission (web service).
Summit Data Platform (SDP)	Customer Experience Data Warehouse (CxDW)	All PATS-R Data is extracted for reporting purposes including Veteran demographics, contact information, enrollment information, eligibility information, service connection, sensitivity, financial assessment information, and insurance.	Encrypted electronic transmission (web service).
Analytics and Business Intelligence LAN	VHA Support Service Center VSSC	All PATS-R Data is extracted for reporting purposes including Veteran demographics, contact information, enrollment information, eligibility information, service connection, sensitivity, financial assessment information, and insurance.	Encrypted electronic transmission (web service).
Identity and Access Management (IAM) - Single Sign-On External (SSOe)	AccessVA	User Identity and Authentication exchanged with AVA web front-end hosted on VA.gov	Encrypted electronic transmission (web service) utilized by PATS-R Sub-System AVA.

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

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

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

Follow the format below:

Privacy Risk: Disclosure of information from a third party.

Mitigation: An Interconnection Security Agreement / Memorandum of Understanding (ISA/MOU) defining the system and data transmission in is in place. Access to the data is limited to appropriate personnel who are required to be trained in the handling of VA PII/PHI and sensitive information.

Privacy Risk: Privacy information may be inadvertently released to unauthorized individuals or the VistA source applications with which the PATS-R application interfaces with may inadvertently release privacy information. If such an instance should occur the impact is considered low.

Mitigation: The PATS-R application ensures strict access to information by enforcing through access control and requirements for end users. Access to the application is by PIV authentication. Individual administrator user IDs and access are provided only based on need. PATS-R limits access rights and controls only to valid end users. Rigorous security monitoring controls are in place to prevent unauthorized access and intrusion, and to protect all information. Furthermore, all end users are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. The VA IT office is responsible in assuring safeguards for the PII.

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***
DoD and Cerner	Joint Electronic Health Record System – Modernized Health Data VA is Adopting	85+ Data Elements related to: Problems, Notes, Orders, Appointments, Medications, Postings, Allergies, Labs, Consults, NonVA Meds, Vitals, Imaging, and Discharges.	Official, signed, Authority to Connect (ATC) within Authority to Operate (ATO).	Read-Only Application Programming Interface (API).

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: PATS-R does not share any data that is being held in the system. Therefore, no privacy risks are associated with sharing information outside of the VA.

Mitigation: There is no information being shared externally and no privacy risks associated with data sharing; therefore, the mitigation strategy is not applicable.

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 VA policy is not to disclose any personal information to third parties outside VA without their consent, except to facilitate the transaction, to act on caller's behalf at their request, or as authorized by law. Any questions or concerns regarding VA privacy policy or use of patient information can be made by contacting via email at Contact VA Privacy Service, or by mailing questions or concerns at Department of Veterans Affairs, Privacy Service, 810 Vermont Avenue, N.W. (005R1A) Washington, DC 20420.

VHA Notice of Privacy Practices is located here.

(Full link for reference: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946).

This Privacy Impact Assessment will be available online as required by the Government Act of 2002, Pub. L. 107–347§208(b)(1)(B)(iii). More detail on privacy policy can be found at VA Privacy Policy at https://www.oprm.va.gov/.

The SORN for PATS-R is as follows:

100VA10H / 86 FR 6988; *"Patient Advocate Tracking System Replacement (PATS-R)—VA"* (Monday, January 25, 2021).

(Full link for reference: https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01501.pdf).

Additionally, the now decommissioned information technology system known as IRIS is being referenced here because the AVA sub-system has replaced the function of IRIS. Legacy IRIS data was migrated into PATS-R in a read-only state. The IRIS SORN is in the process of being updated, and it will be renamed to AVA. Current IRIS SORN is as follows:

151VA005OP6 / 80 FR 27437; *"Inquiry Routing & Information System (IRIS)—VA"* (Wednesday, May 13, 2015).

(Full link for reference: https://www.govinfo.gov/content/pkg/FR-2015-05-13/pdf/2015-11493.pdf).

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

Notice was provided in section 6.1a above.

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.

Patient Advocates and other PATS-R users collect information directly from Veterans, Beneficiaries, and Providers. Patient Advocates inform the patient that the information they have provided is being entered into PATS-R. If the patient asks, notice of what information is required is provided at the time of the interaction. Providers or Personal information from the Veteran or Beneficiary is then populated into the interaction information. The Patient Advocate can then verify with the caller whether the information is correct. The PATS-R application logs all interactions that the Veteran, Beneficiary, or Provider has with the Patient Advocate, the reasons for the contact, and how the Patient Advocate supported the patient. PII, including SSN, DOB, and names, can be saved as part of the interaction.

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.

Veterans have the right to refuse to disclose their SSNs to VHA. The individual is denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (please refer to the: 38 Code of Federal Regulations CFR 1.575(a)). If a patient does not wish to provide their SSN, they may provide their Electronic Data Interchange Personal Identifier (EDIPI). Alternatively, they may provide their First Name, Last Name, and Date of Birth. If the caller does not wish to provide any of this information, there is no denial of service; however, the Patient Advocate will be unable to perform the following actions withing PATS-R:

- Create an interaction within the PATS-R application be routed to another user for action.
- Effectively categorize the interaction type and details.
- Retrieve data from HDR, VES, VSignals and other feeder integration partners.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

The VHA Notice of Privacy Practices explains the rights of the Veteran to request that the VHA restrict the use and/or disclosure of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility maintaining the record.

VHA Notice of Privacy Practices is located here.

(Full link for reference: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946).

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 Patient Advocates / PATS-R users do not provide notice to callers, then they will not know how the information they provide to the PATS-R is being used. The magnitude of impact is low if Veterans and Beneficiaries are not provided this notice because the CSRs are not collecting new data. The Patient Advocates / PATS-R uses are merely verifying authoritative data stored in HDR, VES, VSignals and other feeder systems from where PATS-R pulls data.

Mitigation: Contractor and VA employees are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. In addition, this PIA, which will be available online as required by the eGovernment Act of 2002, Pub. L. 107–347§208(b)(1)(B)(iii), serves to notify Beneficiaries and Providers calling into the Call Center about the collection and storage of personal information.

Privacy Risk: Privacy Information is used or disclosed outside of its intended purpose.

Mitigation: This PIA serves to notify Veterans, beneficiaries and representatives interacting with Patient Advocates / PATS-R users about the collection and storage of personal information. All Veterans, beneficiaries, representatives who are interacting with Patient Advocates / PATS-R users are informed that their information is being entered into PATS-R.

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.***

The VHA Notice of Privacy Practices explains the rights of the Veteran to request access to their records. AVA Form 10-5345a (Individual's Request for a Copy of Their Own Health Information) may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to, and reviewed by, the System Manager for the concerned VHA system of record, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access will be granted.

VHA Notice of Privacy Practices is located here.

(Full link for reference: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946)

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

N/A. System is not exempt.

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.

N/A. PATS-R is a Privacy Act system.

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

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

The VHA Notice of Privacy Practices explains the rights of the Veteran to amend their records. A VA Form 10-5345a (Individual's Request For a Copy of Their Own Health Information), may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the Veteran believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility maintaining the record. A request for amendment of information contained within a system of record must be delivered to the System Manager or their designee for the concerned VHA system of record, and to the facility Privacy Officer or their designee, to be date stamped and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. Individuals have the right to request an amendment (or correction) to information in the PATS-R records if they believe it is incomplete, inaccurate, untimely, or unrelated to operations. The information collected from individuals calling in to PATS-R is used primarily for call tracking, so the information is not typically corrected. Each call is logged individually. If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes those previously provided. The VHA Notice of Privacy Practices also explains the rights of Veterans and Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations.

VHA Notice of Privacy Practices is located here.

(Full link for reference: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946)

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.

In cases where the information in the PATS-R system is inaccurate, Veterans have the right to request amendment or correction of this information in accordance with the Privacy Act and HIPAA Privacy Rule. Individuals have the right to request an amendment (or correction) to their health information in the PATS-R records if they believe it is incomplete, inaccurate, untimely, or unrelated to their care. The individual must submit the request in writing, specify the information that should be corrected, and provide a reason to support the request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility maintaining the Veteran's information. The individual may do any of the following:

- File a *"Statement of Disagreement"*.
- Ask that their initial request for amendment accompany all future disclosures of the disputed health information.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your 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: If individuals are not provided sufficient guidance regarding the access, redress, and correction of their data, then individuals could initiate adverse personnel actions against the Government.

Mitigation: By publishing this PIA, VA makes the public aware of methods for correcting their records. Because this system does not hold authoritative records long-term, it is unlikely individuals will feel the need to correct their information in this system.

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.

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

- Individuals must take and pass training on VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203), and government ethics.
- Individuals must have a completed security investigation.
- After the training and the security investigation are complete, a request is submitted for access.

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

There are no PATS-R users from other agencies; only VA employees are granted access.

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.

There are a total of 26 custom PATS-R and AVA user roles created to allow individuals to view and interact with only the data needed to perform their job duties as they are defined by PATS-R and AVA leadership:

1. PATS-R VPAC
2. PATS-R VISN Organizational Specialist
3. PATS-R VISN Exec
4. PATS-R Service Line User
5. PATS-R Service Level Advocate
6. PATS-R Report Basic
7. PATS-R Report Advanced
8. PATS-R Report Admin
9. PATS-R Provisioning
10. PATS-R Privacy Officer/FOIA User
11. PATS-R Patient Advocate Supervisor
12. PATS-R Patient Advocate
13. PATS-R NSD
14. PATS-R Non-Integrated FOS
15. PATS-R Integration Teams
16. PATS-R Hide Medical Charts
17. PATS-R Facility Organizational Specialist
18. AVA Supervisor
19. AVA Responder
20. AVA Non-FMI Agent
21. AVA Messaging
22. AVA FMI Agent
23. AVA Create Inquiry
24. AVA Call Center Agent
25. AVA Analyst
26. AVA Admin

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.

VA contractors have access to the lower (pre-production) environments for development purposes. Contractors also have access to the upper (live production) environment for maintenance activities. There shall be a regular review of user access to evaluate whether users are active in the environment. If a user is not active, the account will be terminated. A designated VA Project POC is the only person who may submit account creation requests for accountability purposes. Contractor access to the system expires at the end of the contract duration or earlier.

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

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

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

- Contractors must take and pass training on VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203), and government ethics and role-based training based on support role to the system.
- Contractors must have signed the Non-Disclosure Agreement (NDA) and Rules of Behavior (RoB).
- Contractors must have successfully completed VA contractor background security investigation as per the Position Designation Automated Tool (PDT).
- Once complete, a request is submitted for access. Before access is granted to the production environment; this request must be approved by the supervisor, and OI&T Product Manager.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* February 9, 2022
3. *The Authorization Status:* Authority to Operate (ATO)
4. *The Authorization Date:* February 26, 2022
5. *The Authorization Termination Date:* February 28, 2023
6. *The Risk Review Completion Date:* February 26, 2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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.***

N/A.

Section 9 – Technology Usage

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

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

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

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 Cloud Service Provider (CSP) FedRAMP associated with PATS-R is: "Microsoft – Dynamics CRM Online for Government (CRMOL)". The Microsoft Azure Government Contract establishes VA ownership rights of all data including PII. The Contract Number is: 47QTCA22D003G; Task Order: 36C10B22F0089. The Contract's Base Year runs through March 31, 2023.

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.*

The Azure Government General Support Global Operations Services contract establishes VA ownership rights of all data including PII.

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.

The VA Azure Government General Support Global Operations Services contract establishes VA ownership rights of all data. The contract stipulates that the contractor shall not retain any copies of data, in full or in part, at the completion of the performance period. The data shall contain no proprietary elements that would preclude the VA from migrating the data to a different hosting environment or from using a different case management system in the future.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The Azure Government General Support Global Operations Services contract addresses the National Institute of Standards (NIST) 800-144 principle that states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf".

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

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

The use RPAs or "bots" are not implemented within the PATS-R application.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Phillip Cauthers 255139 Digitally signed by Phillip Cauthers 255139
Date: 2023.01.26 09:05:17 -08'00'

Privacy Officer, Phillip Cauthers

Thomas J. Orler 178546 Digitally signed by Thomas J. Orler 178546
Date: 2023.01.26 14:33:09 -06'00'

Information System Security Officer, Thomas Orler

Stefano Masi 474380 Digitally signed by Stefano Masi 474380
Date: 2023.01.26 15:27:29 -05'00'

Information System Owner, Stefano Masi

JOHN WORSHAM (Affiliate) Digitally signed by JOHN WORSHAM (Affiliate)
Date: 2023.01.27 10:53:31 -06'00'

Reviewed for accuracy by PIA Support Analyst

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).

100VA10H / 86 FR 6988; *“Patient Advocate Tracking System Replacement (PATS-R)—VA”* (Monday, January 25, 2021).

(Full link for reference: https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01501.pdf).

151VA005OP6 / 80 FR 27437; *“Inquiry Routing & Information System (IRIS)—VA”* (Wednesday, May 13, 2015).

(Full link for reference: https://www.govinfo.gov/content/pkg/FR-2015-05-13/pdf/2015-11493.pdf).

VHA Notice of Privacy Practices is located here.

(Full link for reference: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946).

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