Privacy Impact Assessment for the VA IT System called:

# Patient Treatment File (PTF)

# Veterans Health Administration (VHA)

# Health Informatics/Health Information Governance

Date PIA submitted for review:

12 May 2023

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Nancy Katz-Johnson | Nancy.katz-johnson@va.gov | 203-535-7280 |
| Information System Security Officer (ISSO) | Griselda Gallegos | Grisleda.Gallegos@va.gov | 512-326-6037 |
| Information System Owner | Temperance Leister | Temperance.Leister@va.gov | 202-270-1432 |

## Abstract

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

This system consists of two applications: Patient Treatment File (PTF) and Medical District Planning (MDP). Every day the VA Medical Centers sends administrative data such as diagnostic and procedural codes for each inpatient discharge from VistA via Mailman to the Data Management Interface (DMI) queue. Weekly data from the PTF application is used as input to the MDP SAS™ files to format data for integration and reporting to the researchers.

The Patient Treatment File (PTF) is the national repository for all Veterans Health Administration (VHA) inpatient admissions and discharges including Community Living Centers. PTF receives data from the VHA Veterans Integrated Systems Technology Architecture (VistA) software. The system incorporates the data transmission using a VA PTF designed record format. Data transmissions are scheduled at medical centers for transmission to the Austin Information Technology Center (AITC). PTF provides reports to the facilities to know which PTF records were accepted or rejected and the associated error(s) for the record rejection. This information is used in VHA to make budget and planning decisions.

## 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 Treatment File (PTF) is the national repository for all Veterans Health Administration (VHA) healthcare inpatient information.

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

1. Patient Treatment File (PTF): PTF application is a core component of the health information architecture of the VHA, providing source data on inpatient treatment and utilization. The PTF application is the primary method used by VA Medical Centers to report inpatient workload, demographics, diagnoses, and treatment information for national analysis. It is also used for program planning, statistical reporting, bed level authorization and adjustment, clinical research and resource planning and allocation. PTF data is transmitted to the Austin Information Technology Center (AITC) and the system includes all the functionality necessary to accept and manage Inpatient Visit Discharge data and transmit the appropriate reports to the facilities. This information is used in VHA to make budget and planning decisions. Each VA Medical Center sends PTF records from their Veterans Integrated Systems Technology Architecture (VistA) software via mailman to the AITC mainframe z13 mainframe PTF application queues. Data Management Interface (DMI) sends those records to the appropriate application for processing. The records pre-processing edits and reports are generated from the AITC z13 mainframe as appropriate. Data is edited for content and reports are created containing to report records received and any errors. The PTF data is put into a master flat file on a

mainframe. PTF data is extracted and put into SAS files/reports on a weekly/quarterly/yearly basis. PTF is batch reporting system, no web-page interface. 2.Medical District Planning (MDP): MDP is the core component, under the PTF accreditation boundary where the data is generated in SAS™ file format for integration and reporting. VHA and Veterans Integrated Service Network (VISN) Support Services Center (VSSC) use this data. The files may be accessed through Time Sharing Option (TSO) on the Austin Information Technology Center (AITC) z/OS base operating system (mainframe). MDP generates weekly, quarterly, and yearly data. The SAS™ files are securely transmitted to the VA Informatics and Computing Infrastructure (VINCI) SAS™ Grid for use in Veterans Health Administration for a VHA wide view of health care and to support health research. MDP is a mainframe batch system, there is no web-page interface.

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

VA Owned and VA Operated

*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.*

There are at least 130 operational VistA systems supporting the delivery of health care in VA.

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

The PTF application is the primary method used by VA Medical Centers to report inpatient workload, demographics, diagnoses, and treatment information for national analysis. It is also used for program planning, statistical reporting, bed level authorization and adjustment, clinical research and resource planning and allocation.

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

PTF data is transmitted to the Austin Information Technology Center (AITC) and the system includes all the functionality necessary to accept and manage Inpatient Visit Discharge data and transmit the appropriate reports to the facilities. This information is used in VHA to make budget and planning decisions. VHA and Veterans Integrated Service Network (VISN) Support Services Center (VSSC) use this data. The files may be accessed through Time Sharing Option (TSO) on the Austin Information Technology Center (AITC) z/OS base operating system (mainframe). MDP generates weekly, quarterly, and yearly data. The SAS™ files are securely transmitted to the VA Informatics and Computing Infrastructure (VINCI) SAS™ Grid for use in Veterans Health Administration for a VHA wide view of health care and to support health research. MDP is a mainframe batch system, there is no web-page interface

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

The PTF System is not operated at more than one site. It is only maintained on the mainframe in Austin and only specific individuals have access to this system.

*3. Legal Authority and SORN*

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

Information in this system is covered by 121VA10A7: National Patient Databases-VA – Authority For Maintenance Of The System: 38 U.S.C 501.

*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?*

N/A

*D. System Changes*

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

No

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

No

## 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)

Zip Code, Age, Date of Death, Current Procedure/Test, Patient Treatment Information, Diagnostic codes, Procedure codes, Surgical Codes, Hospital visits, and Pre-diagnostic Health Data.

**PII Mapping of Components (Servers/Database)**

**Patient Treatment File (PTF)** consists of (1 Key component Mainframe). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Patient Treatment File (PTF) and Medical District Planning (MDP)** 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** |
|---|---|---|---|---|---|
| Medical District Planning (MDP) | Yes | Yes | NAME<br>SSN<br>Date of Birth<br>Date of Death<br>Zip Code<br>Age<br>Previous Medical Records<br>Current Procedure/Test<br>Gender<br>Diagnostic Codes<br>Procedure Codes<br>Surgical Codes<br>Race/Ethnicity<br>Patient Treatment Information<br>Hospital Visits<br>Pre-Diagnostic Health Data | Provided for reporting purposes to OIG*, ARC* and the hospital sites (weekly, monthly, and quarterly) | No users – batch processing only. PIV card and userid/password to access AITC mainframe. |
| Medical District Planning (MDP)<br>Patient Treatment File (PTF) | Yes | Yes | NAME<br>SSN<br>Date of Birth<br>Date of Death<br>Zip Code<br>Age | | |

| | | | | | |
|---|---|---|---|---|---|
| | | | Previous Medical Records<br>Current Procedure/Test<br>Gender<br>Diagnostic Codes<br>Procedure Codes<br>Surgical Codes<br>Race/Ethnicity<br>Patient Treatment Information<br>Hospital Visits<br>Pre-Diagnostic Health Data | | |

* OIG – Office of Inspector General
* ARC – Allocation Resource Center

**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 source of PTF information is from veterans, VA staffs, and non-VA care providers. All information is gathered from the VistA healthcare application Patient Treatment File (PTF). The source of MDP information is predominately from PTF.

*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.*

We only get data from the VA VistA system so not getting data from any commercial or public site.

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

PTF creates Report’s and they get loaded to the EOS Access site where only specific individuals can see reports for their site and they must have the proper security access to even view there sites reports. EAL/TPL, 419 and Census Reports.

**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?*

PTF data is transmitted electronically from VistA via mailman messages through the Data Management Interface (DMI). The social security number is tied to a patient's record. MDP data is securely transmitted electronically from files residing on the VA mainframe at AITC for required processing. The social security number is tied to a patient's record.

*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.*

There is not information provided to PTF on a form it is all provided thru the Mailman messages on the Mainframe.

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

Data is checked daily (since it is transmitted here to Austin daily) for accuracy using the EAL/TPL Reports to show sites what has rejected and needs to be corrected to be accepted.

*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.*

Data is pulled from VA VistA, shared and transmitted to VA applications mentioned in 1.2.

*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.*

Information is being validated and verified throughout the collection, transmission and analysis processes.

**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*

Information in this system is covered by 121VA10A7: National Patient Databases-VA - AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C 501.

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

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

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

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

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

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

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

**<u>Privacy Risk:</u>** The system processes and stores over 2 million records including PII/PHI. Loss of confidentiality could expose the sensitive personal information of veterans to unauthorized/malicious individuals, which would be a violation of the Privacy Act and HIPAA. Consequently, the impact of VA operations, assets, or individuals is expected to be serious.

**Mitigation:** Only personnel with a clear business purpose are allowed access to the system and the information contained within. Consent for use of PII data is signaled by completion and submission of any appropriate form(s) by the Veterans electronically. Safeguards implemented to ensure data is not sent to the wrong organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities.

## 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.*

Name: Veteran's identification, Social Security Number: Used to verify Veteran identity and as a file number for Veteran, Date of Birth: Used to verify Veteran identity, Date of Death: Used to verify date of death, Zip Code: Part of the mailing address, Previous Medical Records: Used to record the history of health and medical conditions of the veterans such as: Health problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, and operations, Current Procedure/Test, Age: Used to determine how old the patient. Gender: Used to identify the patient sex (male or female), Race/Ethnicity: Used to identify patient's race and ethnicity, Diagnostic codes: Used to make short abbreviation notation for different types of diagnostics for physicians to track information, Surgical codes Procedural codes: Used to make short abbreviation notation for different types of procedures, including surgeries for physicians to track information, Patient Treatment Information, Hospital Visits: Used to record patient admissions to the hospitals in the regions across the nations, Pre-diagnostic health data: Used to record pre-diagnostic health data of the patient.

### 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 Patient Treatment File (PTF) is the national repository for all Veterans Health Administration (VHA) healthcare inpatient information. The Patient Treatment File (PTF) and Medical District Planning (MDP) SAS™ Files are the two applications which process veteran inpatient data from daily treatment in all VA hospitals and provide CENSUS quarterly information to the Allocation Resource Center (ARC) and monthly/yearly information to the ARC. These two applications PTF and MDP – use IBM COBOL and SAS™ which are both running on the z/OS base operating system.

*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.*

Every day the VA Medical Centers sends administrative data such as diagnostic and procedural codes for each inpatient discharge from VistA via Mailman to the Data Management Interface (DMI) queue. Weekly data from the PTF application is used as input to the MDP SAS™ files to format data for integration and reporting to the researchers. PTF is the national repository for all VHA healthcare visit/encounter information. PTF receives data from Veterans Health Administration’s (VHA’s) Veterans Integrated Systems Technology Architecture (VistA) software. The system incorporates the data transmission process Health Level Seven (HL7) messaging protocol, allowing exchange of data in standard format. Automating transmission of data between medical facilities and AITC on a scheduled basis, the system includes event-driven reporting techniques, and all of the functionality necessary to accept and manage encounter data, transmit the acknowledgement to the facilities, and provide management reports for tracking and reconciling workload. This information is used in VHA to make budget and planning decisions.

## 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 minimum-security requirements for PTF moderate impact system cover 17 security-related areas regarding protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems.

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

Only individuals that have the proper Security Access to there sites Reports can see the SSN’s and also the individuals here in Austin have to have the proper Security access to be able to see this data.

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

The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

## 2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

*2.4a How is access to the PII determined?*

Access to PII is requested thru IAM for each specific individual requesting to get access to their sites data/reports.

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

I would think the IAM process is the document that would show how they requested access for each individual needing access to the reports.

*2.4c Does access require manager approval?*

Yes, the IAM system where the request is put in at does require different levels of approval before access is granted. They have to request access to the proper Functional Task Code and Read Only Access

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

I would think this would be maintained by the Security or Mainframe system that would be tracking the User Id's that are looking at the date on the Mainframe and EOS Access systems.

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

I would think this is controlled by security since individuals have to request access and get approved before they can even see any of the PII data for their specific site.

## Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

**3.1 What information is retained?**

*Identify and list all information collected from question 1.1 that is* ***retained*** *by the system.*
*This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

NAME, SSN, Date of Birth, Date of Death, Zip Code, Age, Previous Medical Records, Current Procedure/Test, Gender, Diagnostic Codes, Procedure Codes, Surgical Codes, Race/Ethnicity, Patient Treatment Information, Hospital Visits, Pre-Diagnostic Health Data

**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.*

The Veteran's record is to be destroyed upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. Guidelines stated in General Records Schedule (GRS) 5.2, item 020 DAA-GRS-2017-0003-0001. PTF and MDP are data files output from VHA's electronic health record system created for the purpose of information sharing or reference.

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

*An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.*
*This question is related to privacy control DM-2, Data Retention and Disposal.*

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

The records retention schedule is named for its predecessor system, Electronic Document Management System (EDMS) VA. Further details on the EDMS are located at: http://www.rms.oit.va.gov/SOR_Records/92VA045.asp.

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

These records are retained in accordance with the General Records Schedule Sections 3.0 Technology and 4.0 Information Management, approved by National Archives and Records Administration (NARA). http://www.archives.gov/records-mgmt/grs.html The VHA Records Control Schedule (RCS) 10-1 is the main authority for the retention and disposition requirements of VHA records authorized by NARA. It provides a brief description of the records and states the retention period and disposition requirements which can be found at https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf. In accordance with the SORN 2023-07638.pdf (govinfo.gov) National Patient Databases-VA'' (121VA10). Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, General Records Schedule, 5.2, item 020.

### 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.*

Under the jurisdiction of VHA, 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, the General Records Schedule (GRS) and VHA Records Control Schedule (RCS) 10-1. The GRS can be found at www.archives.gov. VA Directive 6300, Records and Information Management contains the policies and responsibilities for VA's Records and Information Management program. VA Handbook 6300.1, "Records Management Procedures", Section 3.2, contains mandatory procedures for the proper management of eliminating data at the end of the retention period. Procedures are enforced by Records management Staff and VA Records Officers. During the last assessment it was found that the organization uses organization-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records)

### 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.*

During the last assessment it was found that the organization develops policies and procedures and implements controls that minimize the use of PII for testing, training and research. AC-1 The organization develops and documents an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The system uses 2FA with PIV and etoken to access servers, PIV and username/password to access AITC mainframe along with special permissions to access data files.AT-1 The organization develops and documents a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to include VA National Rules of Behavior, VA Privacy & Information Security Awareness, and Privacy & HIPAASA-10 For moderate- and high-impact systems, the organization requires that information system developers/integrators perform configuration management during information system design, development, implementation, and operation. They must manage and control changes to the information system, implement only organization-approved changes, document approved changes to the information system, and track security flaws and flaw resolution.SA-11 The information system project manager/developer creates a security test and evaluation plan as part of the implementation phase of a project. The plan is then implemented, and the test results are documented. Systems under development should not process “live data” but utilize de-identified data. Developmental security test results may be used in support of the security A&A process for the delivered information system.

### 3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

*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:*

*<u>Principle of Minimization:</u> 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:
**Privacy Risk:** There is a risk that the information maintained by PTF and MDP could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

**Mitigation:** To mitigate the risk posed by information retention, PTF and MDP adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)." contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting. A toll-free phone number will be established for data breach incidents potentially involving a large (500+) number of individuals. When one occurs the number is activated and posted, along with a Health Information Technology for Economic and Clinical Health (HITECH) Press Release, on the VA Notices web page: http://www.va.gov/about_va/va_notices.asp.

## Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

*Data Shared with Internal Organizations*

| ***List the Program Office or IT System information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| Veterans Health Administration Medical Centers (VHAMC's) | Files created with specific data set names per the setup requests | PTF and MDP data:<br>NAME<br>SSN<br>Date of Birth<br>Date of Death<br>Zip Code<br>Age<br>Previous Medical Records<br>Current Procedure/Test<br>Gender<br>Diagnostic Codes<br>Procedure Codes<br>Surgical Codes<br>Race/Ethnicity<br>Patient Treatment Information<br>Hospital Visits<br>Pre-Diagnostic Health Data | The data is transmitted via Mailman messages from the VistA systems to AITC |
| Veterans Health Administration | Files created with standard data set names per the setup requests | PTF and MDP data:<br>NAME<br>SSN<br>Date of Birth<br>Date of Death | Each VA Medical Center sends PTF extract records from their Veterans Integrated Systems |

| ***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*** |
|---|---|---|---|
| | | Zip Code<br>Age<br>Previous Medical Records<br>Current Procedure/Test<br>Gender<br>Diagnostic Codes<br>Procedure Codes<br>Surgical Codes<br>Race/Ethnicity<br>Patient Treatment Information<br>Hospital Visits<br>Pre-Diagnostic Health Data | Technology Architecture (VistA) software via mailman to the AITC z13 mainframe DMI application queues. |

## 4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

**Privacy Risk:** There is a risk that data contained in EAS may be shared with unauthorized individuals or that those individuals, even with permission to access the data, may share it with other individuals.

**Mitigation:** All users of the system are VA users. All VA users with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. EAS adheres to all information security requirements instituted by the VA Office of Information Technology (OIT). Information is shared in accordance with VA Handbook 6500. Access to veteran data for use is under Title 38 U.S.C Section 5106

## Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

*Data Shared with External Organizations*

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

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

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

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

Follow the format below:

**<u>Privacy Risk:</u>** The potential is the disclosure of information during transmission.

**<u>Mitigation:</u>** Does not share information with external organization.

## 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.*

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946 explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans

receiving care are provided the notice at the time of their encounter. Using VHA fillable form 10-10EZ - A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.
By the system's System of Record Notice (SORN), *Electronic Document Management System (EDMS)-VA,* VA SORN 121VA10, which can be viewed at the following link: [2023-07638.pdf (govinfo.gov)]

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

The sites get a package informing them they now have a Userid and password for the mainframe so they can access the EOS Access site now to view reports for that site.

1. https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
2. https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

*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.*

By this Privacy Impact Assessment, which is available online as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii). By the system's System of Record Notice (SORN), Electronic Document Management System (EDMS)-VA, VA SORN 121VA10, which can be viewed at the following link: 2023-07638.pdf (govinfo.gov)

**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 requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them.

**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 used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR. Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR. Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

### 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:** There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by PTF/MDP prior to providing the information to the PTF/MDP.

**Mitigation:** Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

## 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.***

There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html.

*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 - PTF is not exempt from the Privacy Act

*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.*

Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office. VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

### 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.*

Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D 'Privacy and Release Information, section 8 states the rights of the Veterans to amend to their records via submitting 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 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 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.

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

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

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states: 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. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following: • File an appeal • File a "Statement of Disagreement" • Ask that your initial request for amendment accompany all future disclosures of the disputed health information Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office. Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received

### 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.* ***<u>Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.</u>***
*This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

If no formal redress is provided, you may do any of the following:• File an appeal.• File a "Statement of Disagreement". • Ask that your initial request for amendment accompany all future disclosures of the disputed health
information. http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1089

### 7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

*Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks.* ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

**Privacy Risk:** There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

**Mitigation:** The risk of incorrect information in an individual's records is mitigated by authenticating information, when possible, Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
The NOPP discusses the process for requesting an amendment to one's records.

The*]* Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.
The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

## 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.*

Access to the system is granted to VA employees and contractors by the local authority within each administrative area staff office, following the described account creation process.

*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?*

VA employees and Contractors

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

The sites and individuals here in Austin only have READ Only Access to the Reports out on EOS Access. Office of Information and Technology (OIT) 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 using TMS.

**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 will have access to the system to perform their duties on a need to know basis. Access will be granted after a VA Form 9957 has been filled out and after completion of Security Awareness Training. System follows policies. OI&T provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training for new users, when required by system changes and annually thereafter. Each contract is reviewed prior to approval based on the contract guidelines by the appropriate Contracting Officer's Representative. This Process is conducted each time the individual is hired, or the contract period expires and they were rehired:

- Individuals are subject to a background investigation before given access to Veteran’s information.
- All personnel with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- VA maintains Business Associate Agreements (BAA) and Non-Disclosure Agreements with contracted resources in order to maintain confidentiality of the information.
- Personnel including contractors that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA

Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA’s Talent Management System (TMS). After the user’s initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

**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.*

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB (for AITC technicians) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA’s Talent Management System (TMS). After the user’s initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

**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:* 15 March 2023
3. *The Authorization Status:* Full ATO
4. *The Authorization Date:* 180 Days
5. *The Authorization Termination Date:* 31 May 2023
6. *The Risk Review Completion Date:* 11 April 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

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 System does not use cloud computing.

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

N/A

**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.*

N/A

**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.*

N/A

**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 system does not use RPA.

## 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 they provided in this Privacy Impact Assessment is true and accurate.**

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.06.09 16:31:54 -04'00'

**Privacy Officer, Nancy Katz-Johnson**

Griselda Gallegos 204736

Digitally signed by Griselda Gallegos 204736
Date: 2023.06.16 11:55:08 -05'00'

**Information System Security Officer, Griselda Gallegos**

Temperance M. Leister 3514567

Digitally signed by Temperance M. Leister 3514567
Date: 2023.06.16 13:50:09 -05'00'

**Information System Owner, Temperance Leister**

## 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).

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter**.**

By the system's System of Record Notice (SORN), *Electronic Document Management System (EDMS)-VA,* VA SORN 121VA10, which can be viewed at the following link: 2023-07638.pdf (govinfo.gov)

6.1b Links

1. https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
2. https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

## 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