The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).


Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.
Privacy Impact Assessment for the VA IT System called:

Veterans Personal Finance System (VPFS)
Veterans Health Administration (VHA)

Date PIA submitted for review:
7/6/2020

System Contacts:

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Christian Loftus</td>
<td><a href="mailto:Christian.Loftus@va.gov">Christian.Loftus@va.gov</a></td>
<td>(859) 281-2470</td>
</tr>
<tr>
<td>Information System</td>
<td>Mark McGee</td>
<td><a href="mailto:James.McGee5@va.gov">James.McGee5@va.gov</a></td>
<td>520-629-4834</td>
</tr>
<tr>
<td>Security Officer (ISSO)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information System</td>
<td>Christopher Brown</td>
<td><a href="mailto:christopher.brown1@va.gov">christopher.brown1@va.gov</a></td>
<td>202-270-1432</td>
</tr>
<tr>
<td>Owner</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Abstract

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

Veterans Personal Finance System (VPFS) is the mini-banking system used by the Veterans Health Administration (VHA) to manage the accounts of VHA patients in the VHA hospital system. VPFS is a centralized, web-based, and internally facing application. VPFS stores all data for all sites in one centralized database. Access to the data in the database is controlled by security software that limits access according to your VistA site and user role.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes.
- Whether the completion of this PIA could potentially result in technology changes.
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?
- Does the system use cloud technology? 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.
- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
- 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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?
Veterans Personal Finance System (VPFS) is the mini-banking system used by the Veterans Health Administration (VHA) to manage the accounts of VHA patients in the VHA hospital system. VPFS is maintained by the EPMO/Health Services Portfolio (HSP) office. VPFS is a centralized, web-based, and internally facing application. Access to the data in the database is controlled by security software that limits access according to their VistA site and user role.

VPFS is a centralized system, and all VA sites access the same centralized web application using a browser over the VHA secure Intranet used by VPFS clerks as opposed to a phone application. VPFS is not accessible outside the secure VA Intranet (i.e. it is not web-facing). VPFS is internally VA-hosted and does not use cloud-based technology.

VPFS web/application servers are hosted at Capital Region Readiness Center (CRRC). VPFS stores all data for all sites in one centralized database. The VPFS database is hosted at Austin Information Technology Center (AITC). Access to the application requires a valid two-factor authentication (2FA) PIV/PIN VA identity in order to login. VPFS further limits access to application and its functionality based upon a user’s VistA site and role. VPFS uses VistA secondary menu options and VistA keys to identify user role(s) and restrict user access.

VPFS is VistA integrated, and it allows users to perform PSL (Person Service Lookup) based retrieval of demographic information of Veterans and their dependents. The clerk posts funds that are deposited or withdrawn from the patients’s account. VPFS application keeps track of the account transactions history of the patients. VPFS does not share information to any outside systems. Demographic data is updated in batch (and on-demand / as used) from VistA Financial data within VPFS is manually reconciled by VPFS clerks using its extensive reporting functionality. The information listed below in Section 1.1 is stored in the VPFS database. To date, there are about 984,500 individuals who have their information stored in the database.

VPFS’s Authority to Operate (ATO) was authorized June 4, 2020. It expires December 1, 2020.

The completion of this PIA should not require any changes to the system or the VPFS SORN.

In terms of privacy impact, VPFS stores the Veteran financial information as a standalone banking system. It contains any balance and/or credit afforded the Veteran, as well as stores any transactional data for deposits and credits, as managed by VPFS clerks across the VA.

The VPFS system’s legal authority for operating the system, specifically the authority to collect the information listed is the President’s Executive Order: Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs, including the Federal Advisory Committee Act, as amended (5 U.S.C. App.). Notice is provided by the system’s System of Record Notice (SORN), Electronic Document Management System (EDMS)-VA, VA SORN 79VA10P2 Title 38, United States Code, section 7301(a), and 24VA10P2, that covers Veterans/Dependents, which can be viewed at the following links:

https://www.oprm.va.gov/docs/sorn/SORN79VA10P2.PDF

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.

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:

- [x] Name
- [x] Social Security Number
- [x] Date of Birth
- [ ] Mother’s Maiden Name
- [x] Personal Mailing Address
- [x] Personal Phone Number(s)
- [ ] Personal Fax Number
- [x] Personal Email Address
- [ ] Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- [x] Financial Account Information
- [ ] Health Insurance Beneficiary Numbers
- [ ] Account numbers
- [ ] Certificate/License numbers
- [ ] Vehicle License Plate Number
- [ ] Internet Protocol (IP) Address Numbers
- [ ] Current Medications
- [ ] Previous Medical Records
- [ ] Race/Ethnicity
- [ ] Tax Identification Number
- [x] Medical Record Number
- [x] Other Unique Identifying Number (list below)

Additional Information Collected But Not Listed Above: Physician Name, Claim ID, Claim Number, Gender, Date of Death, Medical information that determines the restriction on the funds or if no restrictions exist, Name of the executor, (Emergency Contact, Beneficiary numbers) Death information, Next to kin in case of death

PII Mapping of Components

VPFS consists of 2 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VPFS and the reasons for the collection of the PII are in the table below.
### PII Mapped to Components

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPFS Database</td>
<td>No</td>
<td>Yes</td>
<td>SSN, DOB, Financial</td>
<td>VPFS manages and reports on Veterans finances</td>
<td>Internally-facing system with an AITC hosted database with restricted and limited access</td>
</tr>
<tr>
<td>Web/Application Server</td>
<td>Yes</td>
<td>No</td>
<td>SSN, DOB, Financial</td>
<td>VPFS manages and reports on Veterans finances</td>
<td>Internally-facing system with a CRRC hosted WebLogic server with restricted and limited access</td>
</tr>
</tbody>
</table>

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

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

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.
The primary data source for VPFS is collected by VPFS clerks interacting with Veterans and entering into the VPFS application. The VPFS clerks also manually reconcile VPFS reports against Financial Management System (FMS) and VistA, which do not have a direct interface with VPFS. The secondary data source for VPFS is collected from existing VistA files. The information is stored locally, viewable nationally, and is based on location.

1.3 How is the information collected?

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

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The PII information is collected via electronic transmission via VistA. Monetary information can be collected via the VPFS clerk through verbal communication with Veterans and/or Dependents.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose.

This question is related to privacy control AP-2, Purpose Specification.

This information is collected to identify the patient as well as manage their financial accounts. The information collected is used manage the accounts of VHA patients in the VHA hospital system, to post deposits or withdrawals made and to maintain the transaction history.
1.5 How will the information be checked for accuracy? How often will it be checked?

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

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

There is a batch job that performs periodic updates to make sure the data from VPFS is timely and up to date. There is also an on-demand job that performs the same service.

Data Quality:

a) VHA takes reasonable steps to confirm the accuracy and relevance of the PII it collects. VHA tries to collect PII directly from the individual whenever possible, which allows for better confirmation of the accuracy, relevant, timeliness and completeness of the information. If information is collected in person verbally or on a VA form this confirmation happens as part of the process. When information is collected online or through the mail, confirmation of PII is handled through other processes, such as computer matches.

b) All PII is reviewed for accuracy as it is collected and utilized to care for Veterans. Any PII identified or determined to be inaccurate or outdated, or erroneously placed in the wrong record by VHA staff is updated administratively immediately as appropriate. VHA will also update any PII in a Privacy Act system of records pursuant to a granted amendment request from the individual. VHA Handbook 1605.1 outlines policy for processing amendment requests. Other policies, such as VHA Handbook 1907.01 outlines how health records are updated including administratively due to errors.

1.6 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 VPFS system’s legal authority for operating the system, specifically the authority to collect the information listed is the President’s Executive Order: Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs, including the Federal Advisory Committee Act, as amended (5 U.S.C. App.). Notice is provided by the system’s System of Record Notice (SORN), Electronic Document Management System (EDMS)-VA, VA SORN 79VA10P2: Title 38, United States Code, section 7301(a), and 24VA10P2: Title 38, United States Code, Sections 501(b) and 304 that covers Veterans/Dependents which can be viewed at the following links:

https://www.oprm.va.gov/docs/sorn/SORN79VA10P2.PDF


1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

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

**Privacy Risk:** The VPFS system collects both Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI) such as social security number. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

**Mitigation:** The VA’s risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall
security controls follow VA 6500 Handbook, and NIST SP800-53 high impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility’s common security controls. These issues are identified and described in the system security plans for the individual information systems.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program’s business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained.
This question is related to privacy control AP-2, Purpose Specification.

The information is internal to VA. It is used to identify the patient, to manage financial information (funds), and includes some medical information for guidance.

The program is used as a ledger to protect the financial interest of the Veteran’s funds that come into our hospitals. VPFS records financial funds deposits by the Veterans. The system maintains data entered by the VPFS clerks, along with the financial deposit information it includes the following:

- Medical information that determines the restriction on the funds or if no restrictions exist
  Used to manage account resources and/or obligations
- Name of the executor: Used to manage account for beneficiaries
- Health provider (doctor or social worker): Used for billing and/or patient representative
- Death date: Used to unassign a patient from his team Next to kin in case of death
- SSN: Used as a patient identifier
- Name: Used as a patient identifier
- DOB: Used to identify patient age and confirm patient identity
- Address: Used to contact the individual
- Phone number(s): Used to contact the individual
- Email: Used to contact the individual
- Financial Account Info: Used to manage resources and obligations
- Physician Name: Used for billing purposes
- Claim ID: Used for billing purposes
- Claim Number: Used for billing purposes
- Gender: Used as a patient identifier
- Next of Kin in case of Death - Used to notify relatives
2.2 What types of tools are used to analyze data and what type of data may be produced?

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

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

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

VPFS users produce several reports in VPFS to compare data between VistA, VPFS, and Financial Management System (FMS). The reports are used to identify appropriation, the amount of the deposits, owner, and the types of transactions completed that day. This is a manual reconciliation of the data to compare information and ensure data accuracy across systems. There is no technical interface or connection between VPFS and FMS.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

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

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.
VPFS users have a tiered access according to their roles and responsibilities. VPFS users must be VA employees. Information Resources Management (IRMs)/Automated Data Processing Application Coordinator (ADPACs) at each site grant users access to VPFS.

The minimum-security requirements for the VPFS system cover multiple related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. 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 facilities employ all security controls in the respective medium 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. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how veterans’ information is used, stored, and protected.

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*

- Medical information that determines the restriction on the funds or if no restrictions exist
  - Used to manage account resources and/or obligations
- Name of the executor: Used to manage account for beneficiaries
- Health provider (doctor or social worker): Used for billing and/or patient representative
- Death date: Used to unassign a patient from his team Next of Kin in case of death
- SSN: Used as a patient identifier
- Name: Used as a patient identifier
- DOB: Used to identify patient age and confirm patient identity
- Address: Used to contact the individual
- Phone number(s): Used to contact the individual
- Email: Used to contact the individual
- Financial Account Info: Used to manage resources and obligations
- Physician Name: Used for billing purposes
- Claim ID: Used for billing purposes
- Claim Number: Used for billing purposes
- Gender: Used as a patient identifier
- Next of Kin in case of Death: Used to notify relatives
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.

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

VPFS stores the patient data indefinitely. There is a mechanism that sets the record as inactive, but the patient record is not removed from the application.

All electronic records are kept indefinitely per Office Inspector General (OIG) guidance. Information stored on electronic storage media are maintained and disposed of in accordance with Records Control Schedule 10–1, Section XLV, as authorized by the National Archives and Records Administration of the United States.

The data retention period has been approved by National Archives and Records Administration (NARA) and is processed according to the following:

Records Control Schedule 10-1 link for VHA: [www.va.gov/vhapublications/rcs10/rcs10-1.pdf](http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf)
National Archives and Records Administration: [www.nara.gov](http://www.nara.gov)

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

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

The data retention period has been approved by National Archives and Records Administration (NARA) and is processed according to the following:

Records Control Schedule 10-1 link for VHA: [www.va.gov/vhapublications/rcs10/rcs10-1.pdf](http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf)
3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc? 
This question is related to privacy control DM-2, Data Retention and Disposal

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. Information stored on electronic storage media are maintained and disposed of in accordance with Records Control Schedule 10–1, Section XLV, as authorized by the National Archives and Records Administration of the United States.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

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 through the use of Talent Management System (TMS). Access to any system for research, testing or training is granted to VA clinical staffs and contractors by the local authority within each administrative area staff office. Only VPFS users during training or testing the application may be using PII, and these VPFS users follow VA policies and procedures to protect PII. Test data is used when testing new or adjusted functionality for application releases. No research is conducted with VPFS.
3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Privacy Risk: All electronic records are kept indefinitely per Office Inspector General (OIG) guidance. The records are kept indefinitely therefore there is a risk of them being unintentionally released.

Mitigation: To mitigate the risk of corruption or deletion posed by information retention, the data is housed in a secure database repository and is backed up by the Information Technology Center operations staff. The risk of unintentional release is mitigated by the enforcement of the security controls on the VPFS systems to limit the access to the data. VPFS follows RCS 10-1 and VB-1 as the NARA approved retention schedules for the system.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veterans Health Administration (VHA) VistA</td>
<td>VPFS receives patient data from VistA to identify the patient.</td>
<td>PII/PHI (SSN, Full Name, Gender, Date of Birth, Date of Death, Address, Phone Number, Email Address, Admission Date, Discharge Date)</td>
<td>VistALink</td>
</tr>
</tbody>
</table>

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

**Privacy Risk:** There is a risk that information may be shared with unauthorized VA program or system or that data could be shared.

**Mitigation:** Safeguards implemented to ensure data is not sent to the wrong VA 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 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: This question is #7 in the Privacy Threshold Analysis.

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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

N/A
5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

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

This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.
Notice is provided by the system’s System of Record Notice (SORN), Veterans Health Information Systems and Technology Architecture 79VA 10P2 and 24VA10P2 that covers Veteran / dependent health information. Links below:

https://www.oprm.va.gov/docs/sorn/SORN79VA10P2.PDF


Section 6 of VHA Directive 1605.01 also ensures individuals receiving care at a VHA facility are provided adequate notice of VHA’s privacy practices. Information Bulletin (IB) 10-163, VHA Notice of Privacy Practices, is provided by the Health Eligibility Center (HEC), along with information on enrollment, to all Veterans enrolling in VHA for the first time. An individual has the right to request a copy of VHA Notice of Privacy Practice at any time. The notice of privacy practices details the uses and disclosures of the individual’s individually identifiable health information that may be made by VHA, as well as the individual’s rights, and VHA’s legal duties with respect to individually identifiable health information.

VHA also provides a copy of the VHA Notice of Privacy Practices (NOPP) to all non-Veteran patients (e.g., humanitarian, non-VA research subjects, caregivers, and Service members receiving care or treatment at a VHA health care facility) at the episode of care when the non-Veteran patient checks in for an appointment or when the non-Veteran patient is admitted to the hospital. All non-Veteran patients must acknowledge receipt of the VHA Notice of Privacy Practices per VHA Handbook 1605.04, Notice of Privacy Practices.

A copy of IB 10-163 can be found on the VHA Publications website at the following link: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3048

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

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

VHA Directive 1605.01 ‘Privacy and Release Information’, section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual’s individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).
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

VHA Directive 1605.01 Privacy and Release Information’, section 11 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual’s individually-identifiable health information to carry out treatment, payment, or health care operations.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

**Principle of Transparency:** Has sufficient notice been provided to the individual?

**Principle of Use Limitation:** Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

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

**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 6 of VHA Directive 1605.01 also ensures individuals receiving care at a VHA facility are provided adequate notice of VHA’s privacy practices. Information Bulletin (IB) 10-163, VHA Notice of Privacy Practices, is provided by the Health Eligibility Center (HEC), along with information on enrollment, to all Veterans enrolling in VHA for the first time. An individual has the right to request a copy of VHA Notice of Privacy Practice at any time.)
Section 7. Access, Redress, and Correction

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

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

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

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

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

VHA Directive 1605.1 Section 7b “Right of Access and/or Review of Records” states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review 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 records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

Veterans with identification can ask VPFS clerks for a copy of their information, and the VPFS clerk will print out a summary, files, or transactions for their review.

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 Directive 1605.1 section 8 “Right To Request Amendment Of Records” 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.

From VHA Directive 1605.01 Section 6 Notice of Privacy Practices (IB 10-163) notification for correcting the information must be accomplished by informing the individual to whom the record pertains by mail. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations whom had previously received the record about the amendment. If 38 U.S.C. 7332-protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations. Request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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

Request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction
Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.

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

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

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

Privacy Risk: There is a risk that the individual accidentally provides incorrect information in their correspondence.

Mitigation: Veterans verbally provide information that is added into VistA at the local VAMC. Any validation performed would merely be the Veteran personally reviewing the information before they provide it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data.
Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

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

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

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

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

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 through the use of Talent Management System (TMS). Access to the system is granted to VA clinical staffs and contractors by the local authority within each administrative area staff office. No other agencies will have access to the VPFS information.

VPFS uses two-factor authentication (2FA) with PIV/PIN, based on the VA’s Identity Access Management Authentication and authorization method.

VPFS also provides role-based access controlled by the use of security keys created for VPFS within VistA. VPFS users obtain access based on their roles and responsibilities. The roles and the level of access each role has, is listed below:

<table>
<thead>
<tr>
<th>Keys</th>
<th>Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRPF_BASIC_OFFICIAL_USER</td>
<td>User has the ability to view selected patient and account information, no reporting privileges.</td>
</tr>
<tr>
<td>PRPF_BASIC_PFC</td>
<td>User has the ability to register patients, search for patients, edit patient information, post transactions, request patient transfers.</td>
</tr>
<tr>
<td>PRPF_LEAD_PFC</td>
<td>User has the ability to register patients, search for patients, edit patient information, post transactions, request and authorize patient transfers.</td>
</tr>
<tr>
<td>PRPF_PFC_SUPER</td>
<td>User has the ability to register patients, search for patients, edit patient information, post transactions, request and authorize patient transfers.</td>
</tr>
<tr>
<td>Keys</td>
<td>Access Level</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>patient transfers, request</td>
<td>application changes through Administration area.</td>
</tr>
<tr>
<td>PRPF_FISCAL_MANAGEMENT</td>
<td>User has the ability to view selected patient and account information, no reporting privileges.</td>
</tr>
<tr>
<td>PRPF_VPFS_SECURITY_ADMIN</td>
<td>User has the ability to view selected patient and account information for purposes of data security.</td>
</tr>
<tr>
<td>PRPF_VPFS_SYSTEM_ADMIN</td>
<td>User has the ability to implement authorized changes to common reference data, no patient record access. <strong>This is a restricted role.</strong></td>
</tr>
<tr>
<td>PRPF_ACCOUNT_OVERDRAWS</td>
<td>User has the ability to overdraw any patient account.</td>
</tr>
<tr>
<td>PRPF_DEFERRAL_OVERRIDE</td>
<td>User has the ability to override deferred transactions.</td>
</tr>
<tr>
<td>PRPF_RESTRICTION_OVERRIDE</td>
<td>User has the ability to override patient restrictions.</td>
</tr>
<tr>
<td>PRPF_DATA_MIGRATION_USERS</td>
<td>User has the ability to migrate legacy Patient Funds data. <strong>This is a restricted role.</strong></td>
</tr>
</tbody>
</table>

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 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.*

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. VA Contractor Rules of Behavior and Non-Disclosure Agreements are a standard annual requirement for VA contractors accessing and supporting VPFS. VPFS clerks are not contractors, but VA employees. The VPFS application Sustainment team has contractors. Based on the nature of the contract, these personnel have access to VPFS PII. These contractors do not have access to the Production system. All individuals are required to take and maintain
their VA training covering NDAs and ROBs. Contracts are monitored and reviewed by the responsible contracting officer on an on-going basis.

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 user must complete, acknowledge, and sign that he/she will abide by the VA Rules of Behavior. The users must complete annual mandatory security and privacy awareness and HIPAA training.

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

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

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

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

1. Signed June 4, 2020
2. Authority To Operate with Conditions (ATOC)
3. 180 days; effective until December 1, 2020
4. Moderate
### Summary of Privacy Controls by Family

#### Section 9. References

**Summary of Privacy Controls by Family**

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

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

CHRISTIAN D LOFTUS 222466
Digitally signed by CHRISTIAN D LOFTUS 222466
Date: 2020.09.10 11:36:58 -04'00'

Privacy Officer, Christian Loftus

James M. McGee 926698
Digitally signed by James M. McGee 926698
Date: 2020.09.10 10:36:38 -07'00'

Information Security Systems Officer, Mark McGee

Christopher Brown 101386
Digitally signed by Christopher Brown 101386
Date: 2020.09.14 16:42:42 -05'00'

Information System Owner, Christopher Brown
APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

Notice is provided by the system’s System of Record Notice (SORN), Veterans Health Information Systems and Technology Architecture 79VA 10P2 and 24VA10P2 that covers Veteran / dependent health information. Links below:

https://www.oprm.va.gov/docs/sorn/SORN79VA10P2.PDF
