SPLASH PAGE LANGUAGE

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).

VA HANDBOOK 6508.1: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," July 2015, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=810&FType=2

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:

Digital Veterans Platform (DVP)

Enterprise Program Management Office

Date PIA submitted for review:

7/16/2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Ron McKelvey	Ron.McKelvey@va.gov	304-596-8357
Information System Owner	David Mazik	David.Mazik@va.gov	732-835-8637

Abstract

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

The Digital Veterans Platform (DVP) is a project under the congressional program called "Other IT Systems Development". The DVP enables secure seamless interoperability between VA and commercial applications, enabling advanced analytics to deliver a cohesive Veteran-centered experience both inside and outside VA.

Overview

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

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

The Digital Veterans Platform (DVP) is a project under the congressional program called "Other IT Systems Development". The DVP enables secure seamless interoperability between VA and commercial applications, enabling advanced analytics to deliver a cohesive Veteran-centered experience both inside and outside VA.

The proposed architecture contains five strategic, integrated components: one Electronic Health Record (EHR), one Operation Management Platform consisting of one resource, financial, supply chain, and human resource system that are integrated seamlessly with the EHR, one Customer

Relationship Management system, one Analytics system, and one open Application Programming Interface (API) gateway that provides seamless interoperability with internal and external systems.

The DVP will allow: VA to integrate more effectively with outside healthcare community and generate greater opportunities for collaboration across the care continuum with private sector providers, effectively shift technology development to commercial EHR and administrative systems vendors that can integrate modular components in the enterprise through open APIs, allowing VA to adopt more efficient and effective management processes, foster an interoperable, active, innovation ecosystem of solutions and services through its API Gateway that contributes to the next generation of care and benefits models, that are evidence-based, tiered and connected across the continuum of engagement, create an open and accessible platform that can be used not only for Veterans, but also for advanced knowledge sharing, clinical decision support, technical expertise, and process interoperability.

The DVP also supports integrations (healthcare and non-healthcare related) between approved VA and BPE applications (e.g., VA Salesforce to backend VA Systems of Record [SOR]), allowing those applications to share information that otherwise would be siloed, lack scalability, require duplication of data, and/or provide inefficient means of data exchange.

The system will only be hosted at one site, the VA-controlled Cloud Computing Environment, Veterans Affairs Enterprise Cloud (VAEC) Amazon Web Services (AWS). The system and data will reside in the VAEC AWS GovCloud environment.

The VAEC and System Owner are ultimately accountable for the security and privacy of data held by a cloud provider. All data will be processed through the VAEC AWS GovCloud environment.

Information is processed by the system through the use of API's. The only Veteran PII/PHI stored at rest within the system are free-form responses to health questionnaires.

The legal authorities to operate the system are 38 U.S.C. 7601-7604 and U.S.C 7681-7683. The system will be covered under the AWS-GovCloud ATO as a Moderate Impact system. (a) Title 40 U.S.C. § 1401 (3), Clinger-Cohen Act of 1996, which directs the development and maintenance of IT architectures by federal agencies to maximize benefits within the federal government (b) Government Performance and Results Act of 1993, designed to improve federal program effectiveness, enhance Congressional decision-making, and strengthen internal controls.

The following VA System of Record Notices (SORNs) applies to DVP system:

- National Patient Databases –VA, SORN 121VA10A7 (Link)
- Patient Medical Records – VA, SORN 24VA10A7 / 85 FR 62406 (Link)
- Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 / 85 FR 84114 (Link)

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:

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

The DVP API Gateway exchanges information between internal VA systems and between internal VA systems and approved (by VA's Project Special Forces) external third-party API consumers. The information exchanged may include Veteran PII and PHI. No PII/PHI will be used in the delivery of health care services supporting direct patient care. This service does not provide or replace the consultation, guidance, or care of a health care professional or other qualified provider. This service provides a supplement for informational and educational purposes only. Health care professionals and other qualified providers should continue to consult authoritative records when making decisions.

Examples of the data exchanged include:

- Veteran address, contact, enrollment, and eligibility information (PII)
- Personal health history (PHI)
- Benefits claims forms (PII and PHI)
- Documents submitted by Veterans or their PoA to substantiate their claims (PII and PHI)

Examples of stored data include:

- The DVP developer portal (https://developer.va.gov) captures basic information (e.g., name, organization, and email address) from application developers (members of the public) interested in using VA's APIs.
- Patient ICN and free form responses on patient health questionnaires submitted by Veterans (PII and PHI).

PII Mapping of Components

Digital Veterans Platform (DVP) consists of **three** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Digital Veterans Platform (DVP)** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

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
dvp-*-developer-portal-users	Yes	Yes	Basic contact information (e.g., name, organization, and email address).	Information is required to register for development (i.e., synthetic data) API keys along with the APIs of interest (e.g., Health, Facilities, Benefits, etc.). There is no validation of this information, so developers are not required to	Data at rest is encrypted using FIPS 140-2 compliant algorithm.

				submit their "real" contact information.	
dvp-*-api-gateway-db	Yes	Yes	Basic contact information (e.g., name, organization, and email address).	Information is required to register for development (i.e., synthetic data) API keys along with the APIs of interest (e.g., Health, Facilities, Benefits, etc.). There is no validation of this information, so developers are not required to submit their "real" contact information.	Data at rest is encrypted using FIPS 140-2 compliant algorithm.
vac10dbsdvp210	Yes	Yes	Patient ICN, potential PII tied to a facility's set of free form responses in patient health questionnaires submitted by Veterans.	DVP is middleware and PII passes through the DVP infrastructure (e.g., as part of a JSON payload delivered by the APIs, accepted as part of a form upload API, etc.). Storage of patient health questionnaires uploaded by veterans using DVP APIs is supported.	Data at rest is encrypted using FIPS 140-2 compliant algorithm.

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.

DVP is middleware and does not create information itself. Information processed or stored by DVP can come from multiple sources through API calls (e.g., allowing Veterans to submit VA forms electronically, as PDFs, via approved applications.). DVP primarily integrates with the VA systems enumerated in in Sections 4 and 5.

1.3 How is the information collected?

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

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

Information is collected and processed through APIs. Information collected and processed will be safeguarded in accordance to VA Handbook 6500 and FIPS 140-2 encryption and data processing standards.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The integrity of the data is based on the integrity controls in place from where the information is requested. All the information will be checked at the source end. Questionnaire forms stored at rest are validated using the Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) Release 4 (R4) Questionnaire Response resource to ensure payload compliance with the spec. The content of the questionnaires is not checked against other sources of information. No PII/PHI will be used in the delivery of health care services supporting direct patient care. Digital Veterans Platform (DVP) APIs do not provide or replace the consultation, guidance, or care of a health care professional or other qualified provider. This service provides a supplement for informational and educational purposes only. Health care professionals and other qualified providers should continue to consult authoritative records when making decisions.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.
This question is related to privacy control AP-1, Authority to Collect

The Digital Veterans Platform (DVP) is a project under the congressional program called "Other IT Systems Development" Supported by the below legal authorities:

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law
- No. 104---231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- E---Government Act of 2002 § 208
- Federal Trade Commission Act § 5
- 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
- Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites
- OMB Memo M---99---18, Privacy Policies on Federal Web Sites
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws
- The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 9397

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: Digital Veterans Platform (DVP) collects and process Personally Identifiable Information (PII), Personal Health Information (PHI), and other data that may identify an individual/Veteran. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.

Mitigation: Data collected and processed by DVP will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. Data stored at rest will be encrypted using 256-bit Advanced Encryption Standard (AES-256). All systems and individuals with access to DVP will be approved, authorized, and authenticated before access is granted by VA Project Manager and System Owner. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

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: Used to identify the Veteran.
Last four digits of Social Security Number: Used as a unique Veteran identifier.
Date of Birth: Used to identify Veteran's age.
Medical Records: Used to collect related Veteran medical records for providers.
Mailing Address: Used for communication with the Veteran.
Phone Number(s): Used for communication with the Veteran.
Email Address: Used for communication with the Veteran.
Mother's Maiden Name: Used to identify the Veteran.
Zip Code: Used to identify the Veteran.
Phone Number(s): Used for communication with the Veteran.
Fax Number: Used for communication with the Veteran.
Email Address: Used for communication with the Veteran.
Emergency Contact Information (Name, Phone Number, etc of a different individual): Used for communication with the Veteran.
Financial Account Information: Used to identify the Veteran.
Health Insurance Beneficiary Numbers: Used to collect information about the Veteran.
Account numbers: Used to collect information about the Veteran.
Certificate/License numbers: Used to collect information about the Veteran.
Vehicle License Plate Number: Used to collect information about the Veteran.
Internet Protocol (IP) Address Numbers: Used to collect information about the Veteran.
Current Medications: Used to collect Veteran's medical information.
Previous Medical Records: Used to collect Veteran's medical information.
Race/Ethnicity: Used to collect information about the Veteran.
Tax Identification Number: Used to identify the Veteran.
Medical Record Number / ICN: Used to identify the Veteran.
Eligibility Information: Used to determine Veteran benefit eligibility information.

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

DVP is middleware and does not create information itself; it exchanges information between internal VA systems and approved (by VA's Project Special Forces) external third-party API consumers. DVP does not utilize tools to analyze accuracy of the source data transmitted through its API Gateway, nor does it perform analysis of any data stored at rest, including the questionnaire forms. The only validation performed on the questionnaires is ensuring payload compliance with the HL7 FHIR R4 Questionnaire Response spec. Analysis or validation of the data exchanged between approved applications and VA backend systems of records through the DVP API Gateway should be validated by the application owners.

The information exchanged by DVP may include Veteran PII and PHI. No PII/PHI will be used in the delivery of health care services supporting direct patient care. This service does not provide or replace the consultation, guidance, or care of a health care professional or other qualified provider. This service provides a supplement for informational and educational purposes only. Health care professionals and other qualified providers should continue to consult authoritative records when making decisions.

2.3 How is the information in the system secured?

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

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

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

Data is encrypted in transit (TLS 1.2+) and DVP utilizes authenticated access to APIs (e.g., API keys, access control lists [ACLs], OAuth 2.0 access tokens, etc.). Data at rest is encrypted using industry standard AES-256 encryption algorithm. No additional SSN-specific protections are implemented by DVP since the information is encrypted in transit using FIPS 140-2 compliant algorithms, and SSNs are not stored at rest.

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

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

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

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

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

The Digital Veterans Platform (DVP) is a Moderate Security Impact system and is hosted in the Amazon Web Services (AWS) GovCloud FedRAMP High classified environment with Trusted Internet Connectivity (TIC).

The DVP API Gateway exchanges information between internal VA systems and approved (by VA's Project Special Forces) external third-party API consumers. To grant access to API consumers, DVP adheres to the principle of least privilege; only granting access to the data requested by the consumer, consented by the veteran, and approved by the System Owner. From a Veteran's perspective, they request access to their own data via an application that integrates with DVP's APIs. Veterans must explicitly consent to share their data with an approved API consumer (application) as part of this process and are also able to revoke this consent. An API key is only issued after the System Owner approves access to the source system. The System Owners are ultimately accountable for the security and privacy of the data in their systems, including PII.

Security controls are in place to ensure data is used and protected in accordance with legal requirements, VA cyber security policies, and VA's stated purpose for using the data. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. The following implementation Privacy Controls that are in accordance with NIST SP 800-53-rev-4:

- Rules Of Behavior
- Two Factor Authentication
- VA Privacy and Security Training
- VA Safeguard and Awareness Training

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
- Organization
- Email Address
- Patient ICN and/or potential PII/PHI tied to a facility's set of free form responses in patient health questionnaires submitted by Veterans.

3.2 How long is information retained?

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

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

DVP adheres to RCS 10-1 for record retention policies (Link), approved by National Archives and Records Administration (NARA). The following RCS 10-1 items are applicable to DVP based on the information retained:

Name, Organization, Email Address:

- 2100.3b – System Access Records - Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. DAA-GRS-2013-0006-0004, item 31.

Patient ICN and patient health questionnaires:

- 6010.3 – Medical Assessment/Forms - Destroy 5 years after being marked for deletion. DAA-0015-2016-0001-0003.

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.

DVP uses the VHA Records Control Schedule (RCS) 10-1, which is approved by the VA records office and NARA. It is the main authority for the retention and disposition requirements of VHA records. It provides a brief description of the records and states the retention period and disposition

requirements. It also provides the NARA disposition authorities or the GRS authorities, whichever is appropriate for the records, in addition to program and service sections.

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

Information stored in DVP lives in databases hosted in the VAEC's AWS GovCloud (FedRAMP High) environment, as listed in section 1.1. Physical media sanitation requirements are inherited from VAEC AWS.

DVP is responsible for implementing retention periods and deletion of information from the databases based on RCS 10-1 and NARA guidance as defined in section 3.2. Information is deleted using a time-based job scheduler that programmatically triggers a cleanup script, which ultimately deletes the records in the database based on the retention criteria.

Rules:
Developer Portal users (Name, Organization, Email Address): Accounts with over 6 years of inactivity are identified and pruned.
Patient ICN and patient health questionnaires: Records flagged for deletion are identified and pruned after 5 years of the deletion flag being set.

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

DVP has pre-production and production environments. During pre-production DVP does not use PII and during the production phase, DVP processes PII.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:
Privacy Risk: There is a risk that the information maintained by DVP 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, DVP adheres to the NARA General Records Schedule, implemented in RCS 10-1. When the retention date is reached for a record, the individual's information is disposed of as defined for each applicable RCS 10-1 item in section 3.4 above.

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 3.10 (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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Veteran-facing Services Platform (VSP)	Data delivery to Veteran-facing and VA applications and acceptance of Veteran information (e.g., Veteran benefit forms [transmitted as PDFs]) from Veteran-facing applications via APIs	Veteran address, contact, enrollment and eligibility, benefits claims forms, documents submitted by Veterans or their PoA to substantiate their claims.	PII/PHI/III processed electronically through encryption via APIs
Exchange Global Address List (GAL)	Synchronization of contacts (VA employees) between the Exchange GAL and VA Salesforce	Basic contact information (e.g., name, organization, email address, and business phone) for VA Employees to be stored as Contacts in VA Salesforce.	Business contact information processed electronically through encryption via APIs
Corporate Data Warehouse (CDW)	Data delivery to Veteran-facing and VA applications via APIs	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) as defined in the FHIR Argonaut Data Query Implementation Guide v1.0. This includes patient name, sex, date of birth, race, ethnicity, preferred language,	SQL Server Connection (Windows authentication/Kerberos)

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 shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		smoking status, problems, medications, medication allergies, laboratory test(s), laboratory value(s)/result(s), vital signs, procedures, immunizations, and health concerns.	
Enrollment System Redesign (ESR)	Data delivery to Veteran-facing and VA applications (e.g., VA Salesforce)	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III). This includes patient eligibility/enrollment information such as associations, insurance and health plans, service-connected disabilities, military service information, preferred facility information, care eligibility, and patient ICN.	PII/PHI/III processed electronically through encryption via APIs
Enterprise Data Warehouse (EDW)	Data delivery to VA applications (e.g., VA Salesforce)	Personally Identifiable Information (PII) and Individually Identifiable Information (III). This includes full name, home address, e-mail, station, work schedule, salary, supervisor, phone number, job title, diagnostics, prescriptions, and claims.	PII/III processed electronically through encryption via SFTP
Master Person Index (MPI)	Data delivery to VA applications (e.g., VA Salesforce)	Personally Identifiable Information (PII) and Individually	PII/III processed electronically through encryption via APIs

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 shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		Identifiable Information (III). This includes identify traits such as full name, social security number, birth sex, date of birth, date of deceased, place of birth city, place of birth state, mother's maiden name, address, and phone number.	
Enterprise Military Information Service (EMIS)	Data delivery to VA applications (e.g., VA Salesforce)	Personally Identifiable Information (PII) and Individually Identifiable Information (III) to determine veteran status. This includes full name, date of birth, social security number, gender, disability rating, and service history.	PII/III processed electronically through encryption via APIs
Financial Services Center (FSC)/Financial Management System (FMS)	Data delivery to VA applications (e.g., VA Salesforce)	Personally Identifiable Information (PII) and Individually Identifiable Information (III) related to caregiver stipend check payments, including name, address, social security number, check eft numbers, and payment amount.	PII/III processed electronically through encryption via SFTP
VA Profile	Data delivery to VA applications (e.g., VA Salesforce)	Personally Identifiable Information (PII) and Individually Identifiable Information (III) related to Veteran and caregiver contact information including	PII/III processed electronically through encryption via APIs

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 shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		home address, phone number, and email.	
Benefits Gateway Services (BGS)	Data delivery to VA applications (e.g., VA Salesforce)	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III). This includes Veteran and caregiver SSN sensitivity, incarceration, power of attorney, fiduciary, aid/attendance, and caregiver status.	PII/PHI/III processed electronically through encryption via APIs
Health Data Repository (HDR)	Data delivery to VA applications (e.g., VA Salesforce)	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) related to read-only patient clinical data. This includes allergies, discharge summary, consultations, flags, laboratory results, medications, notes, orders, problems, radiology, exams, visits, vitals, additional signers, appointments, patient remarks, sensitive patient, VistA users.	PII/PHI/III processed electronically through encryption via APIs
Patient-Centered Management Module (PCMM)	Data delivery to Veteran-facing and VA applications via APIs	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable	PII/PHI/III processed electronically through encryption via APIs

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 shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		Information (III). This includes veteran Patient-Aligned Care Teams (PACT) data.	
VistA	Data delivery to Veteran-facing and VA applications via APIs	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III). This includes patient vital signs, lab results, ICN, and demographics.	PII/PHI/III processed electronically through encryption via APIs

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.

Follow the format below:
Privacy Risk: The privacy risk associate with maintaining PII is that sharing data within the Department of Veterans' Affairs could happen and that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.
Mitigation: The principle of need-to-know is strictly adhered to for DVP support staff. Only support staff with a clear business purpose is allowed access to the system and the information contained within.

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 3.11 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 shared/received 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***
*Approved (by VA Project Special Forces) third-party API consumers	Data delivery to Veteran-facing and VA applications and acceptance of Veteran information (e.g., Veteran benefit forms [transmitted as PDFs]) from Veteran-facing applications via APIs	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III). Depending on the API accessed, the list of data elements varies. This may include full name, date of birth, social security number,	VA API Terms of Service (ToS) / Code of Conduct (CoC)	APIs secured through API keys, Access Control Lists (ACLs), and/or OAuth 2.0 access tokens. Data is encrypted in transit (TLS 1.2+).

		enrollment and eligibility, and benefits claims forms, but can vary based on the API.		
VA Salesforce	Data delivery to VA Salesforce applications	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III). This may include full name, date of birth, social security number, associations, insurance and health plans, and service-connected disabilities, but can vary based on the application.	Memorandum of Understanding (MOU)	Network Access Control Lists (NACLs)
Patient Advocate Tracking System Redesign (PATS-R) via Veterans Relationship Management (VRM) Customer Relationship Management (CRM)	Data delivery to VA Salesforce applications	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III). This includes veteran full name, social security number, date of birth, email, phone, email, gender, ICN, hotline case ID, hotline case status, and case notes.	Memorandum of Understanding (MOU) / Interconnection Security Agreement (ISA)	VRM endpoints are invoked using OAuth 2.0 access tokens. Data is encrypted in transit (TLS 1.2+).

*For an exhaustive list of approved third-party API consumers, please refer to https://github.com/department-of-veterans-affairs/api-coordination/blob/master/APIConsumerOnboarding/production/production-api-list.md

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

The Digital Veterans Platform (DVP) collects and process Personally Identifiable Information (PII), Personal Health Information (PHI), and other data that may identify an individual/Veteran. Information is encrypted in transit. As the DVP resides entirely within VAEC AWS and many of the controls specific to accessing DVP systems (related to the cited OMB Memorandums) are satisfied by VAEC AWS.

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: The privacy risk associated with maintaining PII is that sharing data outside of the Department of Veteran's Affairs could happen and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.
Mitigation: The principle of need-to-know is strictly adhered to for DVP support staff. Only support staff with a clear business purpose is allowed access to the system and the information contained within. In addition, connections to any external content providers are documented in Memorandums of Understanding (MOUs) / Interconnection Security Agreements (ISA) as listed on section 5.1. BPE connections are encrypted in-transit via SSL across our Network Services Operations Center (NSOC)-monitored site-to-site VPN connections. API consumer connections are also encrypted in transit, and each API consumer also agrees to a VA API Terms of Service (ToS) / Code of Conduct (CoC), in addition to undergoing an approval process involving the System Owner as documented in section 2.4. Access controls are in place as dictated by the VA's Risk Management Framework process, following required VA Handbook 6500 and NIST guidelines. Audit log information is forwarded to the Cybersecurity Operations Center (CSOC) for continuous review and monitoring via installed agents by the VA Enterprise Cloud. DVP also has continuous monitoring & alerting in place to detect traffic anomalies and malicious attempts to gain unauthorized access.

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.

The DVP processes information electronically from the systems noted in Sections 4 and 5. DVP is middleware and does not create information itself. Information processed or stored by DVP can come from multiple sources, including the Veteran themselves, through API calls (e.g., allowing Veterans to submit VA forms electronically, as PDFs.). Therefore, DVP does not govern the processes or notices utilized by the content providers to obtain information from individuals.

No PII/PHI will be used in the delivery of health care services supporting direct patient care. Digital Veterans Platform (DVP) APIs do not provide or replace the consultation, guidance, or care of a health care professional or other qualified provider. This service provides a supplement for informational and educational purposes only. Health care professionals and other qualified providers should continue to consult authoritative records when making decisions.

The Benefits Intake API accepts forms, submitted as PDFs. The Benefits Intake API does not automatically place information in VA systems; the forms submitted via the API land in the same place within VA as mailed/faxed forms. As such, the Privacy Act Notice on the forms themselves serves as notice. For the Benefits Claims API, the Veteran is either submitting their information directly (and authenticates/provides consent) or through a Power of Attorney (and authenticates/provides consent on the Veteran's behalf). The Patient-Generated Data (PGD) API accepts and stores information submitted by veterans in free form questionnaires. Questionnaire forms stored at rest are validated using the HL7 FHIR R4 Questionnaire Response resource to ensure payload compliance with the spec. The content of the questionnaires is not checked against other sources of information.

This Privacy Impact Assessment (PIA) also serves as notice of the Digital Veterans Platform (DVP). As required by the eGovernment Act of 2002, Pub.L.107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agencies. VA System of Record Notices (SORNs) which are published in the Federal Register and available online:

- National Patient Databases –VA, SORN 121VA10A7 (Link)
- Patient Medical Records – VA, SORN 24VA10A7 / 85 FR 62406 (Link)
- Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 / 85 FR 84114 (Link)

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 1605.1 section 5 "Individual's Rights" 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 Version Date: October 1, 2017 1.575(a)). Individuals do have an opportunity to decline to provide information at any time. No, there is not a penalty or denial of service for declining to provide information.

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

Individuals have the right to consent to particular uses of information. Individuals are directed to use the Request for Authorization to Release Medical Records Form (VA Form10-5345) describing what information is to be sent out and to whom it is being sent to. Patients have the right to opt-out of VA facility directories.

VHA Directive 1605.1 section 5 "Individual's Rights" 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 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.

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

Follow the format below:
Privacy Risk: There is a risk that VA employees and Veterans will not know that applications built on the DVP processes disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation: The DVP Integrated Project Team (IPT) mitigates this risk by ensuring that it provides individual's notice of information collection and notice of the system's existence through the methods 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?

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.

When requesting access to one's own records, patients are asked to complete VA Form 10-5345a: Individuals' Request for a Copy of their Own Health Information, which can be obtained from the medical center or online at https://www.va.gov/health-care/get-medical-records/

Additionally, Veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the My HealtheVet program, VA's online personal health record. For more information about My HealtheVet at https://www.myhealth.va.gov/index.html
VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 7(b) 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.

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.

In accordance with VHA Directive 1605.1 section 8.a "Right to Request Amendment of Records" states the rights of the Veterans to amend to their records via submitted written request. 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 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.

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 that 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 ensures data accuracy.

The DVP processes information electronically from the systems noted in Sections 4 and 5. Corrections/updates are handled by the source systems of the information. Once approved by the source systems of the information, corrections to patient questionnaires stored in DVP can be performed via the PGD API.

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.

Follow the format below:
Privacy Risk: There is a risk that Veterans whose records contain incorrect information may not receive notification of any changes. Furthermore, incorrect information in a Veteran's record may result in improper identification.

Mitigation: By publishing this PIA the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Virtual VA platform. Furthermore, the SORN provides the point of contact for members of the public who have questions or concerns about applications and evidence files.

The following SORNs are applicable to DVP:

- National Patient Databases –VA, SORN 121VA10A7 (Link)
- Patient Medical Records – VA, SORN 24VA10A7 / 85 FR 62406 (Link)
- Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 / 85 FR 84114 (Link)

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.

All user access to the DVP system will be provisioned and processed in accordance with VA Handbook 6510 (VA Identity and Access Management), which defines the policy and responsibilities to manage identity and access management for the Department of Veterans Affairs (VA) enterprise, and VA Handbook 6500 (Managing Information Security Risk: VA Information Security Program), which provides the risk-based process for selecting system security controls, including the operational requirements for Department of Veterans Affairs (VA) information technology systems. These policies also define the mandatory requirements for annual information security and privacy training for VA employees and contractors, Acknowledging VA Rules of Behavior and Non-Disclosure Agreement (NDA) for contractors who work on the system.

Access to DVP is granted through Common Security Services (CSS). Access is approved by the system owner and by the Information Security Officer (ISO) at the Regional Office at which the employee is located.

To provide access to API consumers, DVP adheres to the principle of least privilege; only granting access to the data requested by the consumer, consented by the veteran, and approved by the System Owner. From a Veteran's perspective, they request access to their own data via an application that integrates with DVP's APIs. Veterans must explicitly consent to share their data with an approved API consumer (application) as part of this process and are also able to revoke this consent. An API key is only issued after the System Owner approves access to the source system. The System Owners are ultimately accountable for the security and privacy of the data in their systems, including PII.

For DVP project team staff, all employees adhere to VA-mandated trainings before accounts are provisioned to access DVP:

- Rules Of Behavior
- Two Factor Authentication
- VA Privacy and Security Training
- VA Safeguard and Awareness Training

Accounts ultimately need to be approved by the System Owner before they are created. Once they do, DVP adheres to project roles maintained by the VAEC mapped back to VA Active Directory groups (e.g. read-only user, project admin, etc.) depending on the employee's role.

Roles:
Read-Only Users: These are users that require access to DVP but don't need modification rights. Users cannot make changes to the underlying application, infrastructure, and content hosted in DVP.
Project Administrators: These are users responsible for maintaining DVP. Users may make changes to the underlying application, infrastructure, and content hosted in DVP.

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.

Contractors will have access to the DVP system. Contracts are reviewed annually by DVP Contracting Officer at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA's TMS. All contractors are cleared using the VA background investigation process and must obtain a Moderate Background Investigation (MBI) clearance before access is granted.
All user access to the DVP system will be provisioned and processed in accordance with VA Handbook 6510 (VA Identity and Access Management), which defines the policy and responsibilities to manage identity and access management for the Department of Veterans Affairs (VA) enterprise, and VA Handbook 6500 (Managing Information Security Risk: VA Information Security Program), which provides the risk-based process for selecting system security controls, including the operational requirements for Department of Veterans Affairs (VA) information technology systems. These policies also define the mandatory requirements for annual information security and privacy training for VA employees and contractors, Acknowledging VA Rules of Behavior and Non-Disclosure Agreement (NDA) for contractors who work on the 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.

Initial and annual Security Awareness Training includes security best practices, threat recognition, privacy, compliance and policy requirements, and reporting obligations. Upon completion of training, personnel must complete a security and privacy quiz with a passing score. All required VA privacy training must be completed in TMS prior to the user being provisioned.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*

6. *The Risk Review Completion Date*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

The System Security Plan is active and was last signed on 15 March 2021. DVP has an active full three-year ATO, which was granted on 27 September 2018 and will be up for renewal on 26 September 2021. The Risk Review was last completed on 1 October 2020. The FIPS 199 classification is MODERATE.

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, 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.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

DVP is middleware running in the VA-authorized and controlled Cloud Computing Environment, Veterans Affairs Enterprise Cloud (VAEC) Amazon Web Services (AWS). The system and data will reside in the VAEC AWS GovCloud environment. VA Enterprise Cloud's AWS platform and associated services leveraged are categorized FedRAMP High.

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

DVP aligns with the Infrastructure as a Service (IaaS) model.

9.3 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

DVP is hosted in VAEC AWS and is covered under the AWS Enterprise Contract. The VAEC and System Owner are ultimately accountable for the security and privacy of data held by a cloud provider. All data will be processed through the VAEC AWS GovCloud environment. This is part of the Shared Responsibility Model for Security in the Cloud (Link).

9.4 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.

No ancillary data is collected.

9.5 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.

This is governed by the Shared Responsibility Model for Security in the Cloud. The application (DVP) is responsible for its data. For all cloud deployment types, the customer owns their data and identities. The customer is responsible for protecting the security of its data and identities, on-premises resources, and the cloud components it controls (which varies by service type).

9.6 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).

DVP does not utilize Robotic Process Automation (RPA) scripts with any databases that contain PII/PHI.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.07.27 15:44:16 -04'00'

Privacy Officer, Rita Grewal

Ronald J. McKelvey 179660

Digitally signed by Ronald J. McKelvey 179660
Date: 2021.07.27 15:49:18 -04'00'

Information System Security Officer, Ron McKelvey

David R Mazik 1751567

Digitally signed by David R Mazik 1751567
Date: 2021.08.04 10:49:44 -04'00'

Information System Owner, David Mazik

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).

Link to the Privacy Policy found here.