Privacy Impact Assessment for the VA IT System called:

# Digital Transformation Center (DTC) Integration Platform (DIP)

# VA Central Office (VACO)

# Health Informatics

# eMASS ID #1480

Date PIA submitted for review:

December 18, 2023

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Lynn Olkowski | Lynn.Olkowski@va.gov | (202)632-8405 |
| Information System Security Officer (ISSO) | Irza Morales | Irza.Morales@va.gov | (787) 772-7301 |
| Information System Owner | Jerry Abernathy | Jerry.Abernathy@va.gov | (202)461-1618 |

## Abstract

*The abstract provides the simplest explanation for "what does the system do?".*

The Digital Transformation Center (DTC) Integration Platform (DIP) is a cloud platform for hosting middleware applications providing interoperability between VA applications to deliver Veteran-centric experience inside the VA. Based in multiple VAEC Virtual Private Clouds (VPC) DIP will provide data transformation and/or translation service between two or more VA applications. The data that passes through the DIP Platform includes PII, PHI, and financial data. As DIP is a platform for middleware applications, it accesses a variety of data from Salesforce and other VA systems. DIP does not act as a System of Record (SOR) for any data. The applications hosted on DIP interact with SORs in order to retrieve data, transform data, and send data.

## Overview

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

*1 General Description*

*A. What is the IT system name and the name of the program office that owns the IT system?*

Digital Transformation Center (DTC) Integration Platform (DIP) is owned by the Office of Information and Health Informatics.

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

The purpose of DIP is to provide a platform for hosting middleware applications that allow internal communication between potentially high-level impact VA applications and approved third party applications.

*C. Who is the owner or control of the IT system or project?*

VA owned and VA operated

*2. Information Collection and Sharing*

*D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?*

DIP does not provide any direct access to end users, but rather serves as a gateway through which internal VA applications can communicate.

*E. What is a general description of the information in the IT system and the purpose for collecting this information?*

DIP typically hosts middleware applications that integrate VA Salesforce modules to other VA Systems, but it can be used as a platform to allow integration between any VA Systems.

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

Data that is handled by the applications hosted on the DIP Platform includes PII, PHI, and financial data.

*G. Is 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?*

DIP resides within the VAEC AWS GovCloud and serves as an internal gateway that can host applications that exchange PII and PHI between VA applications and VA-approved third-party applications.

*3. Legal Authority and SORN*

*H. What is the citation of the legal authority to operate the IT system?*

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

The following VA System of Record Notices apply to DIP:
•Patient Medical Records – VA, SORN 24VA10A7

•Veteran's Health Information Systems and Technology Architecture (VistA) Records – VA,SORN 79VA10

•National Patient Databases –VA, SORN 121VA10A7

*I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

*4. System Changes*

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

Completion of the DIP PIA will not result in any circumstances that require changes to any business processes.

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

Completion of the DIP PIA will not result in any circumstances that require changes to any technology.

## Section 1. Characterization of the Information

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

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

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

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

*The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.*

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☒ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☒ Medical Records
- ☒ Race/Ethnicity
- ☒ Tax Identification Number
- ☒ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Other Data Elements (list below)

Other PII/PHI data elements:

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

DIP acts as a platform for the secure exchange of information, including PII/PHI, between VA Systems and to VA approved external systems such as Salesforce gov cloud. An approved VA System can go through a DIP-hosted middle-ware application hosted on the DTC Integration Platform to retrieve data from other VA systems. DIP may make changes to formatting or perform protocol transformation to data. However, the DIP Platform only allows storage of user data, sensitive personal information (SPI) or otherwise, that is necessary to provide the required middleware capability.

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

The DTC Integration Platform consists of zero key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by DTC Integration Platform and the reasons for the collection of the PII are in the table below.

**Note**: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

*Internal Components Table*

| Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI | Does this system collect PII? (Yes/No) | Does this system store PII? (Yes/No) | Type of PII (SSN, DOB, etc.) | Reason for Collection/ Storage of PII | Safeguards |
|---|---|---|---|---|---|
| N/A | N/A | N/A | N/A | N/A | N/A |

**1.2 What are the sources of the information in the system?**
*These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

*1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?*

DIP is a cloud platform for hosting middleware applications that connect various VA applications and VA approved third-party applications, internally.

*1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.*

DIP will be used to exchange information and provide data and protocol transformation capabilities between applications for user enhancement purposes.

*1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?*

DIP does transmit and receive PII/PHI, but DIP only allows the storage of PII/PHI data for approved use cases and only when necessary to provide the required middleware capability to the VA.

**1.3 How is the information collected?**

*These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

*1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?*

DIP will only exchange information and provide data and protocol transformation capabilities to various VA applications and VA-approved third-party applications.

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

DIP PII/PHI is not collected on a form and is not subject to Paperwork Reduction Act. DIP does transmit and receive PII/PHI, but DIP only allows the storage of PII/PHI data for approved use cases and only when necessary to provide the required middleware capability to the VA.

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

*These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.*

*1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.*

DIP applications receive data only when it is required and only store data within DIP that is necessary to provide the required middleware capability. DIP relies upon the connecting systems to provide valid data and perform their own data integrity checks.

*1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?*

DIP relies upon the connecting systems to provide valid data and perform their own data integrity checks.

**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 DTC Integration Platform (DIP) 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

DIP will also have legal arrangements and agreements for development services, data transformation, configuration management, disaster recovery, incident responses and system continuity plans. DIP does transmit and receive PII/PHI, but DIP only allows the storage of PII/PHI data for approved use cases and only when necessary to provide the required middleware capability to the VA.

**1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information**

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

**Privacy Risk:** There is a risk that PII and/or PHI data could be exposed from the DTC Integration Platform and accessed by individuals who either do not have a need to know or who intend to use the information in a way that is not authorized and is therefore unlawful.

**Mitigation:** DIP hosts applications that provide middleware integration between VA Systems for specific purposes. These applications are purpose-built and provide access only to the information relevant and necessary for the mission. This limits the information that passes through DIP. DIP transmits and receives encrypted PII/PHI data, but DIP only allows the encrypted storage of PII/PHI data for approved use cases and only when necessary to provide the required middleware capability to the VA. When storage does occur, a lifecycle policy is enforced to ensure that the data is stored only for as long as is necessary for the mission. This limits the accessibility of PII and PHI information within the environment. It also means that DIP is always retrieving the latest information from the VA System of Record. DIP does not collect PII or PHI and contains only machine-to-machine interfaces, no direct user interfaces. This means that only individuals that are designated as privileged users, like platform administrators, have direct access to the DIP environment. This limits the individuals who have access to the data.

## 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 that 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.*

| PII/PHI Data Element | Internal Use | External Use |
|---|---|---|
| Name | Used to identify the Veteran | Used to identify the Veteran |
| Social Security Number | Used as a unique Veteran identifier | Used as a unique Veteran identifier |
| Date of Birth | Used to identify Veteran's age | Used to identify Veteran's age |
| Personal Mailing Address | Used for communication with the Veteran. | Used for communication with the Veteran. |

| | | |
|---|---|---|
| Personal Phone Number | | Used for communication with the Veteran. |
| Personal Email Address | Used for communication with the Veteran. | Used for communication with the Veteran. |
| Emergency Contact Information (Name, Phone Number, etc.) | Used for communication with the Veteran. | Used for communication with the Veteran. |
| Financial Account Information | Used to identify the Veteran | Used to identify the Veteran |
| Health Insurance Beneficiary Numbers | Used to collect information about the Veteran | Used to collect information about the Veteran |
| Account numbers | Used to collect information about the Veteran | Used to collect information about the Veteran |
| Certificate/License numbers | Used to collect information about the Veteran | Used to collect information about the Veteran |
| Current Medications | Used to collect information about the Veteran | Used to collect information about the Veteran |
| Race/Ethnicity | Used to collect information about the Veteran | Used to collect information about the Veteran |
| Tax Identification Number | Used to collect information about the Veteran | Used to collect information about the Veteran |
| Tax Identification Number | Used to collect information about the Veteran | Used to collect information about the Veteran |

**2.2 What types of tools are used to analyze data and what type of data may be produced?**
*These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.*

*2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?*

DIP transports (passes through) data and performs protocol and data transformations, but that data is only stored for approved use cases where it is necessary to provide the required capability to the VA.

*2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.*

DIP does not use any tools that are meant to analyze PII/PHI data.

**2.3 How is the information in the system secured?**
*These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.*

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

Application configuration data on DIP is stored in encrypted databases, or as encrypted hashes in configuration files. DIP transmits and receives data through encrypted connections where possible, most commonly using HTTPS/TLS or SFTP connections. All Data at Rest on DIP is stored encrypted.

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

SSNs follow the same rules as other user data: it is transmitted and received on encrypted channels, and it cannot be stored or logged in any way.

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

PII/PHI data is stored only for approved use cases and has lifecycle policies applied that ensure that data is stored for only as long as is necessary.

**2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>**

*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:*

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

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

*2.4a How is access to the PII determined?*
Access to DIP is given to Operations and Maintenance System Administrators, approved users and approved third party administrators for support circumstances by the Information System Owner. DPI also leverages VA Enterprise practices for enabling access to Information Systems or Applications.

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

Access to DIP is given to Operations and Maintenance System Administrators, approved users and approved third party administrators for support circumstances by the Information System Owner. DPI also leverages VA Enterprise practices for enabling access to Information Systems or Applications.

*2.4c Does access require manager approval?*

Access to DIP is given to Operations and Maintenance System Administrators, approved users and approved third party administrators for support circumstances by the Information System Owner. DPI also leverages VA Enterprise practices for enabling access to Information Systems or Applications.

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

Access to DIP is given to Operations and Maintenance System Administrators, approved users and approved third party administrators for support circumstances by the Information System Owner. DPI also leverages VA Enterprise practices for enabling access to Information Systems or Applications.

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

Access to DIP is given to Operations and Maintenance System Administrators, approved users and approved third party administrators for support circumstances by the Information System Owner. DPI also leverages VA Enterprise practices for enabling access to Information Systems or Applications.

## 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*

DIP does not currently store (retain) PII/PHI but does support the capability for middleware applications to persist PII/PHI data for approved use cases. Those data elements consist of: Name, Social Security Number, Date of Birth, Mother's Maiden Name,
Personal Mailing Address, Personal Phone Numbers, Personal Email Address, Emergency Contact Information, Financial Information, Health Insurance Beneficiary Numbers Account numbers, Certificate/License numbers, Medications, Medical Records, Race/Ethnicity, Tax Identification

Number, and Medical Record. DIP allows middleware applications to handle PII/PHI data in the following ways:

1.PII/PHI data may be passed through from one VA System to another (e.g., from VAProfile to Salesforce). This data is not persisted.

2.For approved use cases, PII/PHI data may be temporarily persisted in Encrypted MessageQueues as part of transaction processing.

3.PII/PHI data may be written to application logs. These logs are persisted for only a shorttimeframe and access to these logs is limited to privileged users.

4.For approved use cases, files containing PII/PHI data may be persisted in encryptedstorage on DIP. The use case defines the lifecycle of the data being persisted on DIP andappropriate policies are applied to enforce that lifecycle.

5.For approved use cases, PII/PHI data may be persisted in an encrypted database. The use casedefines the lifecycle of the data being persisted on DIP and appropriate policies are applied toenforce that lifecycle.

**3.2 How long is information retained?**

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.* ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

DIP ensures the appropriate lifecycle of persisted PII/PHI data in the following ways:

1.Data that is written to AWS SQS Queues is deleted as soon as it is used and will be kept for no more than 14 days in any case. Access to the data is restricted to the middleware applications that require the queueing.

2.Application logs that contain PII/PHI data have a lifecycle policy applied that deletes the log data after 45 days. Access to those logs is restricted to authenticated, privileged users and is used for troubleshooting purposes only.

3.Files containing PII/PHI data that are stored on DIP may have lifecycle policies applied that remove files after a predetermined amount of time. The need for the lifecycle policy and the exact amount of time will be determined for each use case. Access to the files is restricted to privileged users (administrators) and to the middleware applications that utilize the data.

4.Databases that contain encrypted PII/PHI data may have lifecycle policies applied that remove records after a predetermined amount of time. The need for this and the exact amount of time will be determined for each use case. Access to these databases is restricted to privileged users and to the middleware applications that utilize the data.

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

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

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

DIP does not directly allow the retrieval of records via personal identifiers. DIP exchanges information and provides data transformation capabilities to connect VA applications and VA approved third-party applications.

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

DIP policy is to retain information for no longer than 6 years, 1 month, and 1 day in accordance with RCS 10-1 link for VHA: http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf.

**3.4 What are the procedures for the elimination or transfer of SPI?**

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

DIP's lifecycle policies are designed to minimize the lifespan of PII/PHI on DIP and automatically purge the data when the lifecycle is complete. "Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin.
https://www.va.gov/vapubs/search_action.cfm?dType=1

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

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

DIP applies lifecycle policies to all instances where PII/PHI data is stored. These lifecycle policies are designed to minimize the lifespan of PII/PHI on DIP and automatically purge the data when the lifecycle is complete.

**3.6 PRIVACY IMPACT ASSESSMENT: Retention of information**

*Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

*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:** Storing PII data for longer than is necessary creates risk of improper exposure of that data.

**Mitigation:** Principle of Minimization: The storage of PII/PHI data is not permitted on DIP except for cases where storage of the data is needed to adequately implement the middleware capability required by the VA. In these cases, the following policies apply:
1.In the case of data that is stored in queues, the data is retained only until used and for no more than 14 days. The data is removed automatically. This policy is set on the queue when it is created and remains in place permanently.

2.In the case of log data that contains PII/PHI data, a lifecycle policy is in place on DIP that automatically deletes log files after 45 days.
3.In the case of files or databases that contain PII/PHI data, the lifecycle of the data will be defined and approved for each use case. In most cases, this will mean that lifecycle policiesare put in place that automatically remove data that exceeds the pre-defined “age”.

**Principle of Data Quality and Integrity:** DIP applies lifecycle policies to all instances where PII/PHI data is stored. These lifecycle policies are designed to minimize the lifespan of PII/PHI on DIP and automatically purge the data when the lifecycle is complete.

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

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

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

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

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

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

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

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

*Data Shared with Internal Organizations*

| ***List the Program Office or IT System information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| VA Centralized Adjudication Background Investigations System (CABS) 2.0 | Data delivery to VA Salesforce applications | • CASE#<br>• E-QIP#<br>• SSN<br>• DOB<br>• ADDRESS<br>• PHONE<br>• E-MAIL<br>• FBI NO.<br>• Request Event User Id<br>• Request Event User IP Address<br>• Request Attachments Agency User Id<br>• Request Attachments User Id<br>• Mother Maiden Name<br>• Citizenship Certificate<br>• Certificate Number<br>• Naturalization Certificate | MOU |
| Exchange Global Address List (GAL) | Synchronization of contacts (VA employees) between the Exchange GAL and VA Salesforce | •Name<br>•Personal Phone Number(s)<br>•Personal Email Address | Business contact information processed electronically through encryption via APIs |
| Veterans Health Administration (VHA), Corporate Data Warehouse (CDW) | Data delivery to VA applications (e.g., VA Salesforce) | •Name<br>•SSN<br>•DOB<br>•Personal Mailing<br>•Personal Phone Number(s) | SQL Server Connection (Windows authentication/Kerberos) |
| Enterprise Data Warehouse (EDW) | Data delivery to VA applications (e.g., VA Salesforce) | •Name<br>•SSN<br>•DOB<br>•Personal Mailing<br>•Personal Phone Number(s)<br>•Personal Email Address<br>•Emergency Contact<br>•Financial AccountInformation | PII/III processed electronically through encryption via SFTP |

| ***List the Program Office or IT System information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| | | •Health InsuranceBeneficiaries Number(s)<br>•Account Number(s)<br>•Certificate/LicenseNumber(s)<br>•Current Medications<br>•Race/Ethnicity<br>•Tax Identification Number(s)<br>•Medical Record Number(s) | |
| Master Person Index (MPI) | Data delivery to VA applications (e.g., VA Salesforce) | •Name<br>•SSN<br>•DOB<br>•Personal Mailing<br>•Personal Phone Number(s)<br>•Personal Email Address<br>•Emergency Contact<br>•Financial AccountInformation | PII/III processed electronically through encryption via APIs |
| Enterprise Military Information Service (EMIS) | Data delivery to VA applications (e.g., VA Salesforce) | •Name<br>•SSN<br>•DOB<br>•Personal Mailing<br>•Personal Phone Number(s)<br>•Personal Email Address<br>•Emergency Contact<br>•Financial AccountInformation<br>•Health InsuranceBeneficiaries Number(s)<br>•Account Number(s)<br>•Certificate/LicenseNumber(s)<br>•Current Medications<br>•Race/Ethnicity<br>•Tax Identification Number(s)<br>•Medical Record Number(s) | 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) | •Name<br>•SSN<br>•DOB<br>•Personal Mailing<br>•Personal Phone Number(s)<br>•Personal Email Address<br>•Emergency Contact<br>•Financial AccountInformation<br>•Health InsuranceBeneficiaries Number(s) | PII/III processed electronically through |

| ***List the Program Office or IT System information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| | | •Account Number(s)<br>•Certificate/LicenseNumber(s)<br>•Current Medications<br>•Race/Ethnicity<br>•Tax Identification Number(s)<br>•Medical Record Number(s) | |
| Office of Information Technology (OI&T), VA Profile | Data delivery to VA applications (e.g., VA Salesforce) | •Name<br>•SSN<br>•DOB<br>•Personal Mailing<br>•Personal Phone Number(s)<br>•Personal Email Address<br>•Emergency Contact<br>•Financial AccountInformation<br>•Health InsuranceBeneficiaries Number(s)<br>•Account Number(s)<br>•Certificate/LicenseNumber(s)<br>•Current Medications<br>•Race/Ethnicity<br>•Tax Identification Number(s)<br>•Medical Record Number(s) | PII/III processed electronically through encryption via APIs |
| Benefits Gateway Services (BGS) | Data delivery to VA applications (e.g., VA Salesforce) | •Name<br>•SSN<br>•DOB<br>•Personal Mailing<br>•Personal Phone Number(s)<br>•Personal Email Address<br>•Emergency Contact<br>•Financial AccountInformation<br>•Health InsuranceBeneficiaries Number(s)<br>•Account Number(s)<br>•Certificate/LicenseNumber(s)<br>•Current Medications<br>•Race/Ethnicity<br>•Tax Identification Number(s)<br>•Medical Record Number(s) | PII/PHI/III processed electronically through encryption via APIs |
| Health Data Repository (HDR) | Data delivery to VA applications (e.g., VA Salesforce) | •Name<br>•SSN<br>•DOB<br>•Personal Mailing | PII/PHI/III processed electronically through |

| ***List the Program Office or IT System information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| | | •Personal Phone Number(s)<br>•Personal Email Address<br>•Emergency Contact<br>•Financial AccountInformation<br>•Health InsuranceBeneficiaries Number(s)<br>•Account Number(s)<br>•Certificate/LicenseNumber(s)<br>•Current Medications<br>•Race/Ethnicity<br>•Tax Identification Number(s)<br>•Medical Record Number(s) | |
| Patient Centered Management Module (PCMM) | Data delivery to VA applications (e.g., VA Salesforce) | •Name<br>•SSN<br>•DOB<br>•Personal Mailing<br>•Personal Phone Number(s)<br>•Personal Email Address<br>•Emergency Contact<br>•Financial AccountInformation<br>•Health InsuranceBeneficiaries Number(s)<br>•Account Number(s)<br>•Certificate/LicenseNumber(s)<br>•Current Medications<br>•Race/Ethnicity<br>•Tax Identification Number(s)<br>•Medical Record Number(s) | PII/PHI/III processed electronically through |
| VDIF, Data delivery to VA applications (e.g., VA Salesforce) | Data delivery to VA applications (e.g., VA Salesforce) | •Name<br>•SSN<br>•DOB<br>•Personal Mailing<br>•Personal Phone Number(s)<br>•Personal Email Address<br>•Emergency Contact<br>•Financial AccountInformation<br>•Health InsuranceBeneficiaries Number(s)<br>•Account Number(s)<br>•Certificate/LicenseNumber(s)<br>•Current Medications<br>•Race/Ethnicity | PII/PHI/III processed electronically through |

| *List the Program Office or IT System information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system* | *Describe the method of transmittal* |
|---|---|---|---|
| | | •Tax Identification Number(s)<br>•Medical Record Number(s) | |
| VistA, Data delivery to VA applications (e.g., VA Salesforce) | Data delivery to VA applications (e.g., VA Salesforce) | •Name<br>•SSN<br>•DOB<br>•Personal Mailing<br>•Personal Phone Number(s)<br>•Personal Email Address<br>•Emergency Contact<br>•Financial AccountInformation<br>•Health InsuranceBeneficiaries Number(s)<br>•Account Number(s)<br>•Certificate/LicenseNumber(s)<br>•Current Medications<br>•Race/Ethnicity<br>•Tax Identification Number(s)<br>•Medical Record Number(s) | 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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

Follow the format below:

**Privacy Risk:** The privacy risk associated 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:** DIP only uses PII/PHI for the authorized purposes identified in the Privacy Act and/or in public notices. Also, the principle of need-to-know is strictly adhered to for DIP support staff. Only support staff with a clear business purpose are 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 3.10 on Privacy Threshold Analysis should be used to answer this question.**

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

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

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

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

*Data Shared with External Organizations*

| ***List External Program Office or IT System information is shared/received with*** | ***List the purpose of information being shared / received / transmitted with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system*** | ***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*** | ***List the method of transmission and the measures in place to secure data*** |
|---|---|---|---|---|
| VA Salesforce | Data delivery to VA Salesforce applications | •Financial Account Information<br>•Health Insurance BeneficiariesNumber(s)<br>•Account Number(s)<br>•Certificate/License Number(s)<br>•Current Medications | 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 | •Name<br>•SSN<br>•DOB<br>•Personal Mailing<br>•Personal Phone Number(s)<br>•Personal Email Address<br>•Emergency Contact<br>•Financial Account Information<br>•Health Insurance BeneficiariesNumber(s)<br>•Account Number(s)<br>•Certificate/License Number(s)<br>•Current Medications<br>•Race/Ethnicity<br>•Tax Identification Number(s)<br>•Medical Record Number(s) | ISA/MOU | VRM endpoints are invoked using OAuth 2.0 access tokens. Data is encrypted in transit using TLS. |
| Defense Counterintelligence and Security Agency (DCSA) | Data delivery to VA Salesforce applications | • CASE#<br>• E-QIP#<br>• NAME<br>• SSN<br>• DOB<br>• ADDRESS<br>• PHONE<br>• E-MAIL<br>• FBI NO. | ISA/MOU | Data is encrypted in transit using TLS. |

| | | | | |
|---|---|---|---|---|
| | | • ACCOUNT<br>• MEMBER NO.<br>• Request Event User Id<br>• Request Event User IP Address<br>• Request Attachments Agency User Id<br>• Request Attachments User Id<br>• Mothers Maiden Name<br>• Citizenship Certificate<br>• Certificate Number<br>• Naturalization Certificate<br>• Certificate Number<br>• US Passport Passport Number<br>• Personal References Name<br>• Personal References Address<br>• Personal References Telephone<br>• Residence History Address | | |

**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.*

*If no External Sharing listed on the table above,* ***(State there is no external sharing in both the risk and mitigation fields).***

*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:** DIP employs a strict need-to-know principle. 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 TLS utilizing the VA's Trusted Internet Connection (TIC). API consumer

connections are also encrypted in transit, and each API consumer also undergoes 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. DIP 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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?**

*These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.*

*6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.*

As a middleware platform, DIP has no user interfaces and does not collect PII/PHI from individuals, only from systems through machine-to-machine interfaces. It will pass PII information between VA Systems, and those Systems provide Privacy Act Notifications.

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

This Privacy Impact Assessment (PIA) also serves as notice of the DTC Integration Platform (DIP). 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:
•Patient Medical Records – VA, SORN 24VA10A7
•Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN79VA10
•National Patient Databases –VA, SORN 121VA10A7

*6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.*

This Privacy Impact Assessment (PIA) also serves as notice of the DTC Integration Platform (DIP). 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.

**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 Handbook 1605.1 Appendix D 'Privacy and Release of 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 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 Handbook 1605.1 Appendix D 'Privacy and Release of 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 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 must be mailed or delivered to the VA health care facility that maintains the record.

**6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>**

*Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

*Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*
*This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.*
Follow the format below:

**Privacy Risk:** There is a risk that VA employees and Veterans will not know that middleware applications hosted on DIP handle Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

**Mitigation:** DIP 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. DIP does not contain user interfaces designed to collect data from individuals.

## Section 7. Access, Redress, and Correction

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

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

*These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.*

*7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions.* ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

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.

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

DIP does not have users nor a user interface for users to request access to, DIP is strictly for administrators with elevated privileges to access command line consoles and therefore this is not applicable.

*7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?*

DIP does not have users, nor does DIP provide access to PII/PHI. DIP serves as a middleware platform connecting VA applications.

**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 Handbook 1605.1 Appendix D 'Privacy and Release of Information', section 8 states the rights of the Veterans to amend to their records via submitted 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.* ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
*This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

DIP facilitates the exchange of Veteran information from between VA Systems; however, DIP stories not the System of Record (SOR) for any of this data. Corrections/updates should be handled in the source systems.

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

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

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

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

*Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?*

*This question is related to privacy control IP-3, Redress.*

Follow the format below:

**Privacy Risk:** There is a risk that 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 DIP:
•Patient Medical Records – VA, SORN 24VA10P2
•Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN79VA10P2
•National Patient Databases –VA, SORN 121VA19

## Section 8. Technical Access and Security

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

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

*These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.*

*8.1a Describe the process by which an individual receives access to the system?*

All user access to DIP is 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 DIP is granted through Common Security Services (CSS). Access is approved by the system owner and by the
*8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?*

Agencies outside the VA do not have access to DIP. DIP does not have users from, nor does DIP provide access permissions to users. DIP serves as middleware platform to connect internal VA applications.

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

DIP does not have users, nor does DIP provide access permissions to users. DIP serves as middleware platform to connect internal VA applications.

**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 can have access to the DIP system. Contracts are reviewed annually by DIP 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 DIP 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.

**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. This training includes but is not limited to the following: Privacy and HIPAA Requirements, Privacy and HIPAA Training, VA Privacy and Information Security Awareness and Rules of Behavior.

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

*8.4a If Yes, provide:*

1. *The Security Plan Status:* Compliant
2. *The System Security Plan Status Date:* 15-Nov-2023
3. *The Authorization Status:* ***Authorized To Operate***
4. *The Authorization Date:* 02-Mar-2023
5. *The Authorization Termination Date:* 02-Mar-2025
6. *The Risk Review Completion Date:* 07-Apr-2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH-HIGH -HIGH

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

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

## Section 9 – Technology Usage

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

**9.1 Does the system use cloud technology? If so, what cloud model is being utilized?**
*If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.*
***Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1****. (Refer to question 3.3.1 of the PTA)*

DIP utilizes the VAEC AWS GovCloud High which has FEDRAMP agency authorization. DIP utilizes the Platform as a Service model via VAEC AWS GovCloud High.

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

These principles are outlined in the AWS GovCloud High contract with the VA and describe ownership of PII/PHI held by AWS with great detail. DIP POCs may be able to provide a relevant artifact upon request.

**9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?**

*Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.*

*This question is related to privacy control DI-1, Data Quality.*

These principles are outlined in the AWS GovCloud High contract with the VA and describe ownership of PII/PHI held by AWS with great detail. DIP POCs may be able to provide a relevant artifact upon request

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

*What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?*

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

These principles are outlined in the AWS GovCloud High contract with the VA and describe ownership of PII/PHI held by AWS with great detail. DIP POCs may be able to provide a relevant artifact upon request

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

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

RPA is not currently applicable to DIP.

## Section 10. References

Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

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

**Signature of Responsible Officials**

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

Lynn A Olkowski

Digitally signed by Lynn A Olkowski
Date: 2024.01.04 07:18:22 -06'00'

**Privacy Officer, Lynn Olkowski**

IRZA MORALES

Digitally signed by IRZA MORALES
Date: 2024.01.08 14:34:47 -04'00'

**Information Systems Security Officer, Irza Morales**

JERRY ABERNATHY

Digitally signed by JERRY ABERNATHY
Date: 2024.01.08 10:14:08 -06'00'

**Information Systems Owner, Jerry Abernathy**

## 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; screen shot of a website collection privacy notice).

## HELPFUL LINKS:

**General Records Schedule**
https://www.archives.gov/records-mgmt/grs.html

**National Archives (Federal Records Management):**
https://www.archives.gov/records-mgmt/grs

**VA Publications:**
https://www.va.gov/vapubs/

**VA Privacy Service Privacy Hub:**
https://dvagov.sharepoint.com/sites/OITPrivacyHub

**Notice of Privacy Practice (NOPP):**
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices