Privacy Impact Assessment for the VA IT System called:

Decision Support System (DSS)

Enterprise Program Management Office (EMPO), VHA Support Service Center (VSSC)

Date PIA submitted for review:

01/13/2022

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)	James Alden	James.Alden@va.gov	781-687-2768
Information System Owner	Temperance Leister	Temperance.Leister@va.gov	484-432-6161

Abstract

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

The Decision Support System (DSS), hosted in Austin Information Technology Center (AITC), is the designated Managerial Cost Accounting (MCA) System of the Department of Veterans Affairs. This system is the Department's only means of complying with Public Laws (e.g., PL 101-576 – the Chief Financial Officers Act of 1990) that mandate the use of a MCA system that can assign costs to the product level. DSS cost data is used at all levels of the VA for important functions, such as cost recovery (billing), budgeting and resource allocation.

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 Decision Support System (DSS) is the designated Managerial Cost Accounting (MCA) System of the Department of Veterans Affairs run by the VA's Managerial Cost Accounting Office (MCAO). The data in DSS is used to calculate and measure the productivity of physicians and other care providers, and to proactively analyze the most cost-effective treatments for high-cost and high-risk patients. This system is the Department's only means of complying with Public Laws (e.g., PL 101-576 – the Chief Financial Officers Act of 1990) that mandate the use of a MCA system that can assign costs to the product level. DSS cost data is used at all levels of the VA for important functions, such as cost recovery (billing), budgeting and resource allocation.

Additionally, the system contains a rich repository of clinical information which is used to promote a more proactive approach to the care of high risk (i.e., diabetes and acute coronary patients) and high cost patients. The data in DSS is also used to calculate and measure the productivity of physicians and other care providers.

Between one and ten million individuals have PII and/or PHI stored in DSS. The Veterans Health Administration Support Service Center (VSSC) maintains a DSS Reports Portal (DSR) from which VA Intranet users may access DSS data in time sequenced arrays of clinical and financial data (or data abstraction to evaluate aggregate data from different viewpoints) and standardized reports. DSS shares information with the following systems:

- Veterans Health Information Systems and Technology Architecture (VistA) databases
- National Patient Care Database (NPCD)
- Financial Management System (FMS)
- VHA Support Services Center (VSSC)
- Patient Treatment Files (PTF)
- Payroll and Accounting Integrated Data (PAID)
- Department of Defense Military Data Repository (MDR)

In order to accurately measure the costs associated with different aspects of patient care, information is collected from Veterans Health Information Systems and Technology Architecture (VistA) databases, the Denver Distribution Center Prosthetics database, the National Patient Care Database (NPCD), Patient Assessment Files, the Alcohol Severity Index, the Post Traumatic Stress Disorder database, Ambulatory Surgery Codes, the Dental Encounter System, the Resident Assessment Instrument, Building the Financial Management System (FMS), VHA Support Services Center (VSSC), Patient Treatment Files (PTF), Payroll and Accounting Integrated Data (PAID), and Department of Defense Military Data Repository (MDR). Between 1 and 10 million individual veterans receiving medical care will have their data in the system.

The legal authority to operate the IT system is Title 38, United States Code § 501

The completion of this PIA will not result in any changes in technology or business processes. The PIA completion will not require changes to the System of Record Notice (SORN).
DSS does not use cloud 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.

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
- ☒ Gender
- ☐ Integration Control Number (ICN)
- ☒ Military History/Service Connection
- ☐ Next of Kin
- ☐ Other Unique Identifying Information (list below)

Zip Code is included but not listed above. Although the veteran's name is not collected, the first four letters of the last name are collected.

PII Mapping of Components

Decision Support System (DSS) consists of 3 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Decision Support System (DSS) and the functions that collect it are mapped below.

PII Mapped to Components

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
Mainframe ApplicationServer1	Yes	Yes	First 4 letters of last name; SSN, Date of Birth, Zip Code, Current Medications, Previous Medical Records, Race/Ethnicity	Cost recovery, budgeting, resource allocation, productivity metrics	Network segmentation; access control lists; least privilege task structure
ApplicationServer2	Yes	Yes	First 4 letters of last name; SSN, Date of Birth, Zip Code, Current Medications, Previous Medical Records, Race/Ethnicity	Cost recovery, budgeting, resource allocation, productivity metrics	Network segmentation; access control lists; least privilege task structure
ApplicationServer3	Yes	Yes	First 4 letters of last name; SSN, Date of Birth, Zip Code, Current Medications, Previous Medical Records, Race/Ethnicity	Cost recovery, budgeting, resource allocation, productivity metrics	Network segmentation; access control lists; least privilege task structure

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.

To accurately measure the costs associated with different aspects of patient care, information is collected from VistA databases, the Denver Distribution Center Prosthetics database, the National Patient Care Database (NPCD), Patient Assessment Files, the Alcohol Severity Index, the Post Traumatic Stress Disorder database, Ambulatory Surgery Codes, the Dental Encounter System, the Resident Assessment Instrument, Building the Financial Management System (FMS), VHA Support Services Center (VSSC), Patient Treatment Files (PTF), Payroll and Accounting Integrated Data (PAID), and Department of Defense Military Data Repository (MDR)

1.3 How is the information collected?

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

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

The information stored in DSS is all collected through electronic transmissions from the source systems listed in section 1.2.

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.

DSS checks source data for accuracy to the extent possible. When it finds potential errors, the DSS site team is notified so that corrective action in the source system can affect repairs. Accuracy checks are performed in the systems where the data is generated – DSS receives data from these systems that have already passed whatever accuracy checks are in place.

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

18 U.S.C. 641 Criminal Code: Public Money, Property or Records,
18 U.S.C. 1905 Criminal Code: Disclosure of Confidential Information
31 U.S. Code § 3512 - Executive agency accounting and other financial management reports and plans,
38 United States Code (U.S.C.) §§ 5721-5728, Veteran's Benefits, Information Security,
38 U.S. Code § 1729A - Department of Veterans Affairs Medical Care Collections Fund, and Public Law 101-576 – the Chief Financial Officers Act of 1990 provide the legal authority for operating the system.
Federal Information Security Management Act (FISMA)
Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:
DSS contains a large amount of PHI and PII, which is necessary to account for costs at the patient encounter level. The compromise of this information would constitute a breach of confidence with the veterans served by VHA.

Disclosure may be made to an agency in the executive, legislative, or judicial branch, or the District of Columbia government in response to its request or at the initiation of VA, in connection with disease tracking, patient outcomes or other health information required for program accountability

Mitigation:
All access is performed through secure internal VA networks, there is no public facing DSS platform. Additionally, most access is limited to non-PII data for large scale reporting. Only selected users, usually clinicians, have access to PII data. All users sign adherence to VA's strict privacy and security controls.

Section 2. Uses of the Information

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

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

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

The data in DSS is used to calculate and measure the productivity of physicians and other care providers, and to proactively analyze the most cost-effective treatments for high-cost and high-risk patients. In order to identify these encounters at the physician and/or patient level, this information must be collected. To differentiate high-risk and high-cost patients, personal information must be collected.

• Name (partial) – identification of patient –internal
• SSN– identification of patient–internal
• Date of Birth (DOB) – identification of patient, statistical analysis and caregiver productivity analysis–internal
• Zip Code – identification of patient, statistical analysis –internal
• Current Medications – treatment analysis and caregiver productivity analysis, statistical analysis –internal Version Date: October 1, 2017 Page 8 of 29
• Previous Medical Records – treatment analysis and caregiver productivity analysis, statistical

analysis –internal
• Race/Ethnicity – statistical analysis –internal

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

The Veterans Health Administration Support Service Center (VSSC) maintains a DSS Reports Portal (DSR) from which VA Intranet users may access DSS data in data cubes and standardized reports. The reporting platform runs using SQL-Server software to build reports. The productivity of clinicians and methods of treatment are measured across different patient populations using cost and outcome data to allow VA to provide the most cost-effective level of care. No new individual information is created in the Decision Support System.

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?

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

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

Data at rest is secured by encrypted data bases; access protected by 2FA and restricted access lists. Access is allowed only via secure, internal VA networks—no outside or external access. Data in-transit is protected by encrypted data circuits and TICs.

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.

Add answer here:

All users of the system take required VA Privacy Training and sign the VA Rules of Behavior. Account management logs are reviewed by the Enterprise Operations Security Access Management and the DSS Version Date: October 1, 2017 Page 9 of 29 Program Managers. System of Record Number (SORN) 121VA10A7 - "National Patient Databases-VA," https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdf explicitly states that the records and information may be used for statistical analysis to produce management reports, for the planning, distribution, and utilization of resources, for workload allocation for patient treatment services, for quality assurance audits, evaluation and employee ratings, and many other uses. As the VA's Management Cost Accounting system that brings together cost and patient treatment data, the uses of information are broad, as described in the SORN. Most DSR users do not have access to the PHI or PII contained in the system but can aggregate data to show overall performance and costs in clinical care. Clinicians and program managers use the data to evaluate and manage their programs.

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 (partial)
• SSN
• DOB
• Zip Code
• Previous Medical Records
• Current Medications
• Race/Ethnicity

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.

All DSS data is retained online for the current year and three prior years at the Austin Information Technology Center. After three years, data is archived on tape, and transferred to a secure federal records facility indefinitely. As stated in the SORN (system of records) all records are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States.

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.

Yes. The following records control schedules are documented in Veterans Health Administration, Records Control Schedule 10-1, dated, November 2017, and approved by NARA: National Archives Job No. N1-015-91-006 “Department of Veterans Affairs”, National Archives Job No. N1-015-91-007, Item 1 “Perpetual Medical Files” and National Archives Job No. N1-015-02-003, Item 6 “Electronic Health Record”.

VHA RCS 10-1 may be found at: https://www.va.gov/vhapublications/index.cfm

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

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission) will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization.

Disposition of Printed Data:
Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014),
https://vaww.va.gov/vapubs/search_action.cfm?dType=2

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), https://vaww.va.gov/vapubs/search_action.cfm?dType=2
When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1.
Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

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

All IT system and application development and deployment are handled by VA OI&T. VHA does test new or modified IT systems for VHA operations prior to deployment, and PII/PHI may be used for that Alpha or Beta testing at the facility-level per VHA policy. In addition, VHA may need to train staff on functionality in the new or modified IT system. Training, including on IT systems, is part of health care operations and per VHA policy PII and PHI may be used for that training purpose. However, VHA must minimize the use of PII and PHI in training presentations or materials per VA policy and directives (VA Directive 6511, Directive 6507, Handbook 6507.1 VHA Handbook 1605.1).

VHA minimizes where feasible the risk to privacy of using PII for training and research by following VA policy and performing privacy reviews as necessary. VA OI&T must address risk to privacy regarding testing per their software quality assurance processes.

A risk minimization method is that authentication is required to reach any of the DSS components and their respective data. All access is approved before connectivity.

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:

The risk is that the longer the data is kept, the greater the risk of inadvertent disclosure or a breach. The result of a breach could cause great personal and financial harm to the individual and adversely impact the VA's public image.

Mitigation:
All DSS data is retained online for the current year and two prior years at the Austin Information Technology Center. After three years, data is archived on tape, and transferred to a secure federal records facility indefinitely. All access is initiated through secure internal VA networks, there is no public facing DSS platform. Site teams who access the system have access to cost, workload, and PII data. All users sign adherence to VA's strict privacy and security controls.

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.
Strata (DSS System Vendor)
AITC

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***
Internal Organization Name	**IT System Name**	**Data Elements**	**Method of Transmission**
VHA Office of Finance	Decision Support System- Reporting (DSR)	DSS Reporting-(DSR) collects and stores the following patient specific information from DSS: last name (first 4 characters), SSN, birthdate, race/ethnicity, zip code, previous medical records, current medications.	Files are downloaded from the mainframe via SFTP or SAS/Connect.
VA wide	VistA (electronic medical records system used in VHA)	These extracts provide clinical workload and patient identification data not otherwise available in central VHA databases and include patient and encounter demographic data from VistA clinical systems: appointments, admissions, discharges, movements, laboratory, pharmacy, radiology, surgery, speech and audiology, chaplain, social work, nutrition, and others.	MCA site team staff pull 17 extracts from each local VA medical center VistA system and transmit them to AITC in the form of e-mail messages
VHA, National Data Systems	NPCD (National Patient Care Database in AITC)	These extracts provide MCA with the official VHA encounter data. The records contain patient demographic data and data about each encounter such as provider, date/time, diagnosis, and procedures.	The extracts are created by the NPCD staff in AITC and transmitted to MCA processing on the AITC mainframe through the local AITC LAN.
VHA, National Data Systems	PTF (National Patient Treatment File in AITC)	These extracts provide MCA with the official VHA inpatient admission & discharge data. The records contain patient demographic data and data	The extracts are created from the SAS files generated by the PTF staff in AITC for their

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*
		about each inpatient admission such as provider, date/time, diagnosis, and procedures.	downstream users. They are pulled into MCA processing from the AITC Mainframe
VA OI&T	CDW (Corporate Data Warehouse contains extracted VistA data as well as files from many other sources)	MCA extracts dental workload data from CDW. This workload is not available anywhere else as a central database. The records contain patient demographic data and data about each dental encounter such as provider, date/time, diagnosis, and procedures.	The extract is created on CDW workspace, transferred to a MCA AITC mainframe file and then pulled into MCA processing
VHA. Geriatrics and Extended Care, Office of Patient Care Services	RAI/MDS (Resident Assessment Index/Minimum Data Set database in AITC)	These extracts provide MCA with the patient Condition assessments for Community Living Center patients which are posted to MCA encounters for long-term care patients. The records contain only enough patient data to link the record to the already-existing MCA inpatient encounter record. They contain the assessment scores and dates.	The extracts are created by the RAI/MDS staff in AITC and transmitted to MCA processing on the AITC mainframe through the local AITC LAN.
VA Denver Acquisition & Logistics Center (DALC), Office of Acquisition and Logistics (OAL)	DALC (Denver Logistics and Acquisition Center and their database)	This extract provides MCA with the prosthetic issue records for items mailed to the patient and/or mailed to clinics within VHA medical centers. The records patient data and details about the prosthetic item. Separate records detail mailings to medical center clinics.	Monthly DALC transmits the extract through secure FTP to MCA processing on the AITC mainframe.
VHA Office of Public Health, Occupational Health, Safety, and	OHRS (Occupational Health Record	This extract provides MCA with the clinical workload data not available in other systems.	Monthly OHRS transmits the extract through secure FTP

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*
Prevention Strategic Health Care Group (VHA Occupational Health)	Keeping System is a web-based application that is replacing current methods of recording employee health care in VistA)	The records patient data and details about the office visit such as provider, date/time and procedure.	to MCA processing on the AITC mainframe.
HR & Payroll Application Services	Personnel and Accounting Integrated Data (PAID)	PII and payroll data First 4 letters of last name; SSN, Date of Birth, Zip Code, Current Medications, Previous Medical Records, Race/Ethnicity	Files are created on the AITC mainframe by PAID and then loaded and processed by DSS. There is no transmission of data outside of the mainframe.

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:

DSS contains a large amount of PHI and PII, which is necessary to account for costs at the patient encounter level. The compromise of this information would constitute a breach of confidence with the veterans served by VHA.

Mitigation:

Access control for DSS is very limited for PII and PHI. The data already exists in the other systems without DSS, and the electronic transfers of information are secure. All access is done through secure internal VA networks, there is no public facing DSS platform. Additionally, most access is limited to non-PII data for large scale reporting. Only selected users, usually clinicians, have access to PII data. All users sign adherence to VA's strict privacy and security controls.

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***
Department of Defense (DoD) Defense Information System Agency (DISA) Military Data	Process clinical data collected for those active duty personnel who receive medical assistance at the	Social Security, Date of Birth, Current Medications, Previous Medical and Race/Ethnicity	Federal Information Security Management Act (FISMA) VA Directive 6500, Managing Information Security Risk: VA Information Security Program, and Handbook	Connect Direct Virtual Public Network (VPN) connection

Repository (MDR)	Federal Health Centers		6500, Risk Management Framework for VA Information Systems: Tier 3 – VA Information Security Program Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, Security Guide for Interconnecting Information Technology Systems 38 United States Code (U.S.C.) §§ 5721-5728, Veteran's Benefits, Information Connect Direct Virtual Public Network (VPN) connection Security Office of Management and Budget (OMB) Circular A-130, Appendix III, Connect Direct Virtual Public Network (VPN) connection Version Date: October 1, 2017 Page 17 of 29 Security of Federal Automated Information Systems 18 U.S.C. 641 Criminal Code: Public Money, Property or Records	

			18 U.S.C. 1905 Criminal Code: Disclosure of Confidential Information DoD Instruction 4000.19, Inter-service and Intragovernmental Support, 9 Aug 1995 DoD Directive 8500.01E, Information Assurance (IA)," 24 Oct 2002 DoD Instruction 8500.2, Information Assurance (IA) Implementation, 6 Feb 2003 DoD Instruction 8510.01, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Application Manual, 28 Nov 2007 DoD 6025.18-R, DoD Health Information Privacy Regulation	

To protect veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:

1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.

4. Internal protection is managed by access controls such as user IDs and passwords, authentication,
awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

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:
Sharing data outside of the Department of Veteran's Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation:
The System Interconnect Agreement/Memorandum of Understanding is being routed for signatures. This document defines the terms and conditions for sharing the DoD data with the VA. No VA information is shared outside the VA – the interface only brings DoD information into the VA.

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.

No notice is provided by DSS. No information is collected from the veteran by DSS. Any notice given to the veteran informing him or her that PHI and/or PII would be collected would be given by the source systems that collect the information from the veteran and feed DSS with information. System of Record Number (SORN) 121VA10A7 - "National Patient Databases-VA," https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdf

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

No opportunity or right to decline to provide information is provided by DSS. No information is collected from the veteran by DSS. Any opportunity or notice of the right to decline to provide information given to the veteran would be given by the source systems that collect the information from the veteran and feed DSS with 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

Any right for the individual to consent to particular uses of their information would be handled by the source systems that collect the information from the veteran and feed DSS with information.

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.

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

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

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

Follow the format below:
Privacy Risk:
There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by DSS.

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

Section 7. Access, Redress, and Correction

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

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

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.

As written in SORN 121VA10A7, available at https://www.federalregister.gov/documents/2018/02/12/2018-02760/privacy-act-of-1974-system-of-records.pdf Individuals seeking information regarding access to and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Information Technology Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at 512–326–6780.

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.

There are no provisions for correcting inaccurate or erroneous information in DSS. The information in DSS is all obtained via interfaces with source systems. If there is erroneous or inaccurate information, it should be addressed in those source systems.

The respective source system of records' PIA for their procedures for information correction are at https://www.oprm.va.gov/privacy/pia.aspx
As written in SORN 121VA10A7, available at https://www.federalregister.gov/documents/2018/02/12/2018-02760/privacy-act-of-1974-system-of-records.pdf Individuals seeking information regarding access to and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Information Technology Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at 512–326–6780.

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.

As written in SORN 121VA10A7, available at https://www.federalregister.gov/documents/2018/02/12/2018-02760/privacy-act-of-1974-system-of-records.pdf Individuals seeking information regarding access to and contesting of records in

this system may write or call the Director of National Data Systems (10P2C), Austin Information Technology Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at 512–326–6780.

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.

There are no provisions for correcting inaccurate or erroneous information in DSS. The information in DSS is all obtained via interfaces with source systems. If there is erroneous or inaccurate information, it should be addressed in those source systems.

An alternative for the individual would be to follow the directions in the SORN of this system or the directions of the SORN for the source systems supplying data to DSS.

The SORN for this system states: Individuals seeking information regarding access to and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Information Technology Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA National Service Desk and ask to speak with the VHA Director of National Data Systems at (512) 326–6780.

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:
Without a means of correcting erroneous information, there is a risk that erroneous information is placed into DSS via the interfacing systems. There is a risk that individuals may seek to access or redress records about them held in DSS and become frustrated with the results of their attempt.

Mitigation:
There are no provisions for correcting inaccurate or erroneous information in DSS. The information in DSS is all obtained via interfaces with source systems. If there is erroneous or inaccurate information, it should be addressed in those source systems.

The individual can contact the VA using the directions in the SORN which will lead to a correction in the source system's data.

The SORN for this system states: Individuals seeking information regarding access to and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Information Technology Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA National Service Desk and ask to speak with the VHA Director of National Data Systems at (512) 326–6780.

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.

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.
OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records. This documentation and monitoring is performed using VA's Talent Management System (TMS). Access is granted by submitting a 9957 form with appropriate functional task codes to MCA Program staff, who grant system access.

There are four types of users that have access to DSS:

• IO staff assigned to maintain DSS on the mainframe
• Programmers who maintain the software
• MCA Program Staff who maintain the system, provide assistance to site teams, and extract data needed for reports, etc.
• VHA site staff who process the data for their sites.

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.

Contract staff employed by MCA for DSS support, IO staff assigned to maintain DSS on the mainframe, or VHA sites to process data for their sites can obtain access by the same process as VA Full Time Employees. The process contract review is not within the purview of the DSS application, it is within the responsibility of the VA offices hiring contractors.

VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually 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 Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background

investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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

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

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete Privacy and HIPAA Focused training annually.

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.***

DSS Security Plan Status is approved, with Security Plan Status date of December 2, 2021. Completed A&A process and was granted a 365 DAY ATO on February 26, 2021. The ATO is valid

until March 12, 2022, with Risk Review Completion Date of February 24, 2022. The FIPS 199 classification of the system is High

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).

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.

N/A

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)

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

N/A

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

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

audit trails, and other such metadata that is generated and accumulated within the cloud environment.

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

N/A

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

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

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

N/A

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

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

N/A

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 provided in this Privacy Impact Assessment is true and accurate.

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2022.02.23 14:11:22 -05'00'

Privacy Officer, Rita Grewal

JAMES B. ALDEN 201589

Digitally signed by JAMES B. ALDEN 201589
Date: 2022.02.23 08:48:08 -05'00'

Information Systems Security Officer, James Alden

Temperance M. Leister 3514567

Digitally signed by Temperance M. Leister 3514567
Date: 2022.02.14 15:07:23 -07'00'

Information Systems Owner, Temperance Leister

APPENDIX A-6.1

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

Link to VA Privacy Website: https://www.va.gov/privacy/ .

Link to VHA Notice of Privacy Practices:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3048.

System of Record Number (SORN) 121VA10A7 - "National Patient Databases-VA,"
https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdf