Privacy Impact Assessment for the VA IT System called:

Data Access Services (DAS)

VACO Administration

VA OIT Product Engineering Service, Veterans Experience Services Portfolio

eMASS ID # 773

Date PIA submitted for review:

November 21, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov OITPrivacy@va.gov	202-632-8431
Information System Security Officer (ISSO)	Eric Abraham	Eric.Abraham@va.gov	512.326.7422
Information System Owner	John Tirrell	John.tirrell@va.gov	973.518.3977

Abstract

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

The Data Access Services (DAS) system enables the secure exchange of Veteran, Service Member, and Patient medical, benefits, and administrative data between internal VA Partners [Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), National Cemetery Administration (NCA), Office of Information & Technology (OIT), and Office of Electronic Health Records Modernization (OEHRM)] and external systems, including the Department of Defense (DoD), the Cerner Federal Enclave, the Centers for Medicare and Medicaid Services (CMS), as well as non-Federal partners.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

DAS delivers a wide range of integrally linked, complementary capabilities and services that enable the exchange of Veteran and Service Member medical, benefit, personnel, and personal/administrative information. These capabilities cut across the entire VA enterprise, including Veterans Health Administration (VHA), Veterans Benefit Administration (VBA), National Cemetery Administration (NCA), and Office of Information Technology (OIT) program offices, and in many cases, external partners, such as DoD, as well as non-federal partners.

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

VA Office of Information Technology

2. Information Collection and Sharing

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

The expected number of individuals, Veterans, and Service members whose information is stored in the system is more than 10 million and will continue to increase.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☐	VA Employees
☐	Clinical Trainees
☐	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

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

Veteran and Service Member medical, benefit, personnel, and personal/administrative information. These This data supports the benefit adjudication process as well as patient treatment/healthcare.

E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

DAS is a common access mechanism to exchange and store Veterans' electronic record information from inside and outside of the VA. Consumers initiate all data transactions/requests and, in response, the DAS system aggregates the response data from multiple Producers to provide to the Consumers. The components of DAS that serve as the document repository are MongoDB and AWS S3.

F. Are the modules/subsystems only applicable if information is shared?

yes

G. Is the system operated in more than one site to include primary and secondary 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?

DAS is operated in VAEC AWS and Azure GovClouds. All application and security configurations are consistent across both environments. The singular datastore for PII is located in VAEC AWS GovCloud

3. Legal Authority and System of Record Notices (SORN)

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

Title 38 United States Code (U.S.C), Section 501 and Sections 901–905. The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act."

H. What is the SORN?

168VA005 Health Information Exchange–VA, https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf

I. *SORN revisions/modification*

The above SORN is not under revision or modification.

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*

No updates are required to the SORN

4. System Changes

J. *Will the business processes change due to the information collection and sharing?*

☐ *Yes*
☒ *No*
if yes, <<ADD ANSWER HERE>>

K. *Will the technology changes impact information collection and sharing?*

☐ *Yes*
☒ *No*
if yes, <<ADD ANSWER HERE>>

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 Information 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

☒ **Full** Social Security Number
☒ **Partial** 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/Sex
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Date of Death
☐ Business Email Address
☒ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (list below)

Other PII/PHI data elements: Claim number

1.2 List 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?

- VBA Contracted Vendors, DoD, VA systems to support compensation and pension and claims adjudication.
- Community Care Networks, DoD and VA systems to support healthcare related activities.
- VHA Contract Vendors to support healthcare activities as it relates to oncology.
- State correctional facilities for identification of Veteran population with institution.

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.

All data received is from the authoritative source.

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

DAS does not create any information.

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

1.3 Methods of information collection

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?

All data is received via electronic transmissions from producers/authoritative sources of the data.

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?

This information is not collected on a paper form and is not subject to the Paperwork Reduction Act.

1.4 Information checks for accuracy, and 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.

Some of the information is submitted from existing VA systems, and the accuracy is verified by the original source. Data is checked for completeness by system audits, manual verifications, and annual questionnaires through automated veteran letters. These letters ask specific questions for verification based on the existing entitlement or benefit the veteran is receiving. The correspondence with each veteran is then used to update the data manually. All collected data are matched against supporting claims documentation submitted by the veteran. Certain data, such as a Social Security Number (SSN), is verified with the Social Security Administration. Data is received via Connect Direct to/from SSA. Prior to any award or entitlement authorization(s) by the VBA, the veteran record is manually reviewed, and data validated to ensure correct entitlement has been approved.

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?

This system does not check for accuracy by accessing a commercial aggregator of information.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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 applicable legal authority falls under: SORN 168VA005, Title 38 United States Code (U.S.C), Section 501 and Sections 901–905. The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act."

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: The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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: DAS is a middleware system that enables intra- and inter-agency data transport, transformation and storage capabilities between data producers and data consumers that is inclusive of veteran PII and PHI. This transfer of this data via the DAS system is necessary to maintain a veteran’s electronic health record, or for financial and supportive documentation. If this information were to be breached, then it would cause a direct negative impact to veterans, their families, as well as the any other entities that are stated within the data transfers.

Mitigation:DAS employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. DAS utilizes VA OIT, OIS and ECSO dictated guidelines inclusive of ISA/MOU documentation, access control restrictions, incident response/handling, regular security scans with prompt and timely remediation and network restrictions. Any findings deemed inappropriate are terminated and the system is tracked with several monitoring mechanisms to protect the critical data transferred. DAS also performs both tabletop and real time incident response testing to ensure that the system and the system team are fully capable and prepared to address any potential breach to reduce or eliminate any unauthorized disclosure of 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	Veteran/Patient Identification purposes	Veteran/Patient Identification purposes
Mailing Address	Veteran/Patient communication purposes	Veteran/Patient communication purposes
Phone Number	Veteran/Patient communication purposes	Veteran/Patient communication purposes
Email	Veteran/Patient communication purposes	Veteran/Patient communication purposes
Claim Number	Veteran/Patient Identification purposes	Veteran/Patient Identification purposes
Social Security Number, full and Last 4	Veteran/Patient Identification purposes	Veteran/Patient Identification purposes
Date of Birth	Veteran/Patient Identification purposes	Veteran/Patient Identification purposes
Internal Control Number	Veteran/Patient Identification purposes	Veteran/Patient Identification purposes
Electronic Data Interchange Personal Identifier (EDIPI)	Veteran/Patient Identification purposes	Veteran/Patient Identification purposes
Medical Records	Used to record current health and medical conditions of the Veteran, such as: health problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, and operations.	Used to record current health and medical conditions of the Veteran, such as: health problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, and operations.
Medications	To order meds, check medications currently in use by patient, fulfill medication requests and report for PDMP.	To order meds, check medications currently in use by patient, fulfill medication requests.

2.2 Describe the types of tools 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?

DAS is hosted in VAEC AWS GovCloud and utilizes AWS tools (Opensearch, Lambda functions) to respond to user queries for data, both structured and unstructured, stored within AWS S3 and MongoDB.

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.

Any new available data will create a new record in the DAS datastore which is linked to any existing records for that transaction or veteran of interest.

2.3 How the information in the system is 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?

All data at rest and in transit is encrypted.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

All SSNs are encrypted at rest and in transit.

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

All data at rest and in transit is encrypted.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

<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?

A role-based access control (RBAC) security approach is used to limit users only to the information needed to do their job and prevent them from accessing information that doesn't pertain to them. Only DAS system personnel have direct access to the DAS datastore and the data within; user roles and Active Directory user groups exist in the system. Data owners are responsible for authorizing access to PII and leverage the safeguards implemented by DAS DevSecOps. IT systems requiring access much have a valid need approved by the business owner for the data.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Data owners are responsible for authorizing access to PII and leverage the safeguards implemented by DAS DevSecOps. IT systems requiring access much have a valid need approved by the business owner for the data.

2.4c Does access require manager approval?

Data owners are responsible for authorizing access to PII and leverage the safeguards implemented by DAS DevSecOps.

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

DAS maintains audit logs for all system/data access.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

The DAS System team is responsible for ensuring that all safeguards are implemented to protect PII.

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, Social Security Number (full/partial), Date of Birth, Personal Mailing address, Personal Phone number, Personal email address, medical records, medications, claim number, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

Destruction of Technology Management records is authorized when the data is 5 years old or when it is no longer needed for business use, whichever is longer. For Health record data destruction is authorized once it has been confirmed to be added to the Electronic Health Record.

3.3 The retention schedule 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. Please work with the system 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?

Yes

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

These records are retained in accordance with the General Records Schedule Sections 3.1 General Technology Management Records items 010, 011, 020,030, 040, Section 3.2 Information Systems Security Records items 030, 031, 035, 036, and Section 4. Information Access and Protection Records items 020, 030, 031; and VHA Records Control Schedule 10-1_ approved by National Archives and Records Administration (NARA) Job No. N1-15-02-3 Section 1006 Information Access and Protection Records items 1006.1a, 1006.1b, 1006.2, 1006.3, 1006.4, 1000.5, Section 6000 Health Information Management Service item 6000.2. [http://www.archives.gov/records-mgmt/grs.html.](http://www.archives.gov/records-mgmt/grs.html)

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.

All Electronic Records are deleted from the information systems according to the VA Standard operating Procedure-Media Sanitization and Disposition, GRS or VHA RCS 10-1 NARA disposition instructions.

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.

The DAS system only utilizes test data for testing purposes. All test data has been approved by the Privacy Office prior to use. This system is not used for training or research.

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 Privacy Officer (PO) 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: *The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by DAS could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, DAS adheres to the NARA General Records Schedule. When the retention date is reached for a record, the individuals' information is carefully disposed of by the determined method as described in General Records Schedule Sections 3.0 Technology and 4.0 Information Management. http://www.archives.gov/records-mgmt/grs.html.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a DAS consists of two key component (application service which includes database/storage). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by DAS and the reasons for the collection of the PII are listed 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 3.9a 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**
DAS MongoDB	Yes	Yes	Name, Social Security Number (full/partial), Date of Birth, Personal Mailing address, Personal Phone number, Personal email address, medical records, medications, claim number, Internal Control Number and Electronic	DAS delivers a wide range of integrally linked, complementary capabilities and services that enable the exchange of Veteran and Service Member medical, benefit, personnel, and personal/administrative information. DAS collects and stores information for two main purposes: 1. Bidirectional Exchange of structured and unstructured information within the VA and other provider partners. 2. Correlation of patient identities between VA and other provider partners including the	Role-based access granted through the Elevated Privileges Access System (EPAS). •Data is encrypted at rest and in transit.

			Data Interchange Personal Identifier (EDIPI).	Department of Defense (DoD).	
DAS AWS S3 Storage	Yes	Yes	Name, Social Security Number (full/partial), Date of Birth, Personal Mailing address, Personal Phone number, Personal email address, medical records, Medications, claims number, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI)	DAS delivers a wide range of integrally linked, complementary capabilities and services that enable the exchange of Veteran and Service Member medical, benefit, personnel, and personal/administrative information. DAS collects and stores information for two main purposes: 1. Bidirectional Exchange of structured and unstructured information within the VA and other provider partners. 2. Correlation of patient identities between VA and other provider partners including the Department of Defense (DoD).	Role-based access granted through the Elevated Privileges Access System (EPAS). •Data is encrypted at rest and in transit.

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
VBA–Veteran Benefit Management System (VBMS)	VBMS and VBA work with DAS to provide storage, transport, and validation of exam requests and Disability Benefits Questionnaires (DBQs) and Service Treatment Records (STRs).	Name, Personal Mailing Address, Personal Phone number, Personal Email, Claim number, Social Security Number, Date of Birth, Medical Records, Medications, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VBA-Compensation and Pension Record System (CAPRI)	CAPRI, VBMS and VBA work with DAS to provide storage, transport, and validation of exam requests and Disability Benefits Questionnaires (DBQs).	Name, Personal Mailing Address, Personal Phone number, Personal Email, Claim number, Social Security Number, Date of Birth, Medical Records, Medications, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VBA-Veteran Information/ Eligibility Reporting System (VIERS)	DAS transports data to VIERS to determine a Veteran’s eligibility status and ACA status.	Name, Personal Mailing Address, Personal Phone number, Personal Email, Claim number, Date of Birth, Medical Records, medications, Internal Control Number and Electronic Data	HTTPS using SSL encryption and Certificate exchange.

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		Interchange Personal Identifier (EDIPI).	
VHA-Direct Secure Messaging (DSM)	Secure email portal with external providers that stores attachments in DAS.	Name, Personal Mailing Address, Personal Phone number, Personal Email, Claim number, Date of Birth, Medical Records, Medications, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VHA-Legacy Viewer Sustainment (LVS)	DAS transports DoD data to LVS for clinical use.	Name, Personal Mailing Address, Phone number, Personal Email, Date of Birth, Medical Records, Medications, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VHA-Joint Viewer Sustainment (JLV)	DAS retrieves Oracle Cerner data for JLV for clinical use.	Name, Personal Mailing Address, Personal Phone number, Personal Email, Claim number, Date of Birth, Medical Records, Medications, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VHA-Central VistA Image Exchange (CVIX)	Bi-Directional exchange with DoD for Veteran health data.	Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Medical Records, Medications, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VHA-Veteran Re-Entry Search Service (VRSS)	DAS sends a CSV file provided by external facilities to determine if an individual has served in the military.	Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth.	HTTPS using SSL encryption and Certificate exchange.

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
VHA-Veteran Health Information System and Technology Architecture (VistA)	Application used to connect/write data to VistA.	Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Medical Records, Medications, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VHA – Corporate Data Warehouse (CDW)	CDW sends partner health data to DAS for long term storage.	Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Medical Records, Medications, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VHA-Enrollment Systems Community Care (ESCC)	Sends Veteran eEligibility and demographic information to community care contract vendors for purpose of clinical care and store eligibility documentation.	Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VA-Veterans Data Integration and Federation (VDIF)	Prescription drug monitoring program reporting data and telehealth management records.	Name, Medical Records, Medications, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VHA-VistA ePrescribing (eRX)	Submission of prescriptions with external VHA-contracted vendors.	Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Medical Records, Pharmacy Records, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VA-Federal Case Management Tool (FCMT)	Sharing of interagency comprehensive continued care plans	Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Medical	HTTPS using SSL encryption and Certificate exchange.

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
	with DoD for continued care of veterans.	Records, Medications, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	
VA-Identity and Access Management (IAM)	Used for patient ID correlation, known facilities list and integrated login.	Name, Date of Birth, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VA-National Precision Oncology Program (NPOP)	Oncology documents and image retrieval submitted by external vendors.	Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Medical Records, Medications, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VA-Provider Profile Management System (PPMS)	Provider profile information for VA providers to support scheduling and network management functions.	Name, Personal Phone number, Personal Email.	HTTPS using SSL encryption and Certificate exchange.
VHA-Community Care Referrals and Authorizations (CCRA)	Referrals, authorizations, and storage of community care related data.	Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Medical Record, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VA-Enterprise Program Reporting System (EPRS)	Reporting capabilities for community care data submitted by external vendors.	Name and Medical Record.	HTTPS using SSL encryption and Certificate exchange.
VHA-Community Care Reimbursement System (CCRS)	Submission of NCPDP files for community administered care.	Name, Date of Birth, Medical Record, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VHA-Dental Record Manager (DRM)	Routing of dental records between VA and Cerner clinicians.	Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Protected Health Information, Internal	HTTPS using SSL encryption and Certificate exchange.

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		Control Number and Electronic Data Interchange Personal Identifier (EDIPI), Medical Records.	
VHA-Beneficiary Travel Self Service System (BTSSS)	Routing of self-service travel data.	Name, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI).	HTTPS using SSL encryption and Certificate exchange.
VHA-InteleRad	Routing of appointments and medical order messages between Oracle Cerner, VistAs, and VA site InteleRad PACS.	Name, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI), Medical record.	HTTPS using SSL encryption and Certificate exchange.
VHA-TeleICU	Routing of clinical data and notes for TeleICU consults.	Name, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI), Medical Record.	HTTPS using SSL encryption and Certificate exchange.
VHA – Behavioral Health Lab (BHL)	Routing of clinical data and reports to Oracle Cerner.	Name, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI), Medical Record.	HTTPS using SSL encryption and Certificate exchange.
VHA – Clinical Assessment, Reporting and Tracking (CART)	Routing of clinical data and reports to Oracle Cerner.	Name, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI), Medical Record.	HTTPS using SSL encryption and Certificate exchange.
VHA – My HealtheVet (MHV)	Routing of clinical data, secure messages, pharmacy records and reports to Oracle Cerner.	Name, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI), Medical Record.	HTTPS using SSL encryption and Certificate exchange.
VBA Automation Platform	Routing of clinical data from Oracle Cerner to support for claims adjudication.	Name, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI), Medical Record.	HTTPS using SSL encryption and Certificate exchange.
VHA – VA HealthConnect CRM	Retrieve/Create encounters, retrieve/write notes to	Name, Internal Control Number and Electronic Data Interchange Personal	HTTPS using SSL encryption and Certificate exchange.

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
	VistA and Oracle Cerner.	Identifier (EDIPI), Date of Birth and Medical Record	
BedMasterEX	Routing of ADTs, ORUs and ORMs between Oracle Health and VAMCs.	Name, Internal Control Number and Electronic Data Interchange Personal Identifier (EDIPI), Date of Birth and Medical Record	HTTPS using SSL encryption and Certificate exchange.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in 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 Veteran's Affair could happen, and that the data may be disclosed to individuals who do not require access which heightens the threat of the information being misused

Mitigation: The principle of need-to-know is strictly adhered to by DAS personnel. Only personnel 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
OptumServe Health Services (formerly LHI)	OptumServe Health Services provides medical disability examinations for Veterans with claims being evaluated by the VA's VBA. OptumServe generates a report of the exam results, which is electronically transferred to the VA. Additionally,	Both directions. Name, Personal Mailing Address, Personal Phone number, Personal Email, Claim number, Date of Birth, Medical Records, Pharmacy Records, Patient Identifier.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.

	Optum acts as a community care network provider and sends/receives provider, referral, and claims data.			
Quality, Timeliness, Customer Service Management Inc. (QTC) System	QTC provides medical disability examinations for Veterans with claims being evaluated by the VA’s VBA. QTC generates a report of the exam results, which is electronically transferred to the VA.	Both directions. Name, Personal Mailing Address, Personal Phone number, Personal Email, Claim number, Date of Birth, Medical Records, Pharmacy Records, Patient Identifier.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.
Veterans Evaluation Services (VES) System	VES provides medical disability examinations for Veterans with claims being evaluated by the VA’s VBA. VES generates a report of the exam results, which is electronically transferred to the VA.	Both directions. Name, Personal Mailing Address, Personal Phone number, Personal Email, Claim number, Date of Birth, Medical Records, Pharmacy Records, Patient Identifier.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.
Tyler Technologies	Tyler Tech provides software as a Claims Management System to Veteran’s Service Organizations (VSO’s).	Both directions. Name, Personal Mailing Address, Personal Phone number, Personal Email, Claim number, Date of Birth, Medical Records, Pharmacy Records, Patient Identifier.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.
The Change Healthcare ePrescribing (eRx)	Verifies and transmits eRx transactions to/from external provider (Electronic Health	Both directions. Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Medical	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.

	Record) EHR systems and the VA Infrastructure, i.e., DAS system.	Records, Pharmacy Records, Patient Identifier.		
HAIMS (Healthcare Artifacts and Image Management System)	DoD system with which DAS sends and receives Veteran health data/artifacts.	Both directions. Name, Personal Mailing Address, Personal Phone number, Personal Email, Claim number, Date of Birth, Medical Records, Pharmacy Records, Patient Identifier.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.
DMIX Exchange Service / Department of Defense (DoD)	DoD system with which DAS sends and receives Veteran health data/artifacts.	Both directions. Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Medical Records, Pharmacy Records, Patient Identifier.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.
Tri-West System	Tri-West acts as a community care network provider and sends/receives provider, referral, and claims data.	Both directions. Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Protected Health Information, Patient Identifier.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.
Centers for Medicare and Medicaid Services (CMS) System	This is a bidirectional service with VA to determine health coverage/eligibility.	From CMS to DAS. Name, Date of Birth, Patient Identifier.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.
Foundation Medicine Inc. (FMI) System	Oncology documents and image submission to VA.	From FMI to DAS. Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Medical Records, Pharmacy Records, Patient Identifier.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.
Interqual Inc. System (Change Healthcare)	Generic medical procedure data to determine treatment plans.	From Interqual to DAS. No PHI/PII.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.
DoD Case Management	Sharing of interagency comprehensive	Both directions. Name, Personal Mailing Address, Personal Phone	ISA/MOU	HTTPS using SSL encryption

System (DoD CMS)	continued care plans with VA for continued care of veterans.	number, Personal Email, Date of Birth, Medical Records, Pharmacy Records, Patient Identifier.		and Certificate exchange.
Cerner Federal Enclave (OpenLink, Rhapsody, FHIR Ignite, Citrix, LILA, 3M HSP, JHIE, Secure Messaging, CAMM)	Exchange of data for veteran care and benefits.	Both directions. Name, Personal Mailing Address, Personal Phone number, Personal Email, Claim number, Date of Birth, Medical Records, Pharmacy Records, Patient Identifier.	ISA/MOU	HTTPS/MLLP using SSL encryption and Certificate exchange.
Life Image Inc System	DICOM images for patient care.	From Life Image to DAS. Name, Date of Birth, Medical Records to include Images, Patient Identifier.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.
Prevention Genetics System	Oncology documents and image submission to VA.	From PG to DAS. Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Medical Records, Pharmacy Records, Patient Identifier.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.
Loyal Source Government Solutions System (LSGS)	LSGS provides medical disability examinations for Veterans with claims being evaluated by the VA's VBA. LSGS generates a report of the exam results, which is electronically transferred to the VA.	Both directions. Name, Personal Mailing Address, Personal Phone number, Personal Email, Claim number, Date of Birth, Medical Records, Pharmacy Records, Patient Identifier.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.
Tempus	Oncology documents and image submission to VA.	From Tempus to DAS. Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Medical	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.

		Records, Pharmacy Records, Patient Identifier.		
Logicoy	VA is required by federal law to report all controlled substance prescriptions to the state’s Prescription Drug Monitoring Program (PDMP)	Name, Personal Mailing Address, Personal Phone Number, Date of Birth, Pharmacy Records, Patient Identifier	AO Authorized Memo and POAM	Secure File Transfer
Valor	HL7 messages to support clinical care to/from Oracle Cerner.	Name, Date of Birth, Health Records, Patient Identifier.	ISA/MOU	MLLP using SSL encryption and Certificate exchange.
Fulgent	Oncology documents and image submission to VA.	From Fulgent to DAS. Name, Personal Mailing Address, Personal Phone number, Personal Email, Date of Birth, Medical Records, Pharmacy Records, Patient Identifier.	ISA/MOU	HTTPS using SSL encryption and Certificate exchange.

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

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

*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 increase the risk that data may be disclosed to individuals who do not require access which heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by DAS personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system. The System Interconnect Agreement/Memorandum of Understandings are in place. These documents define the terms and conditions for sharing the data to and from the VA. Safeguards are implemented to ensure data is not sent to the wrong organization, program, or system. VA employees, contractors, and business partners take security, awareness, and privacy training and are required to report suspicious activity. Use of secure passwords, access for need-to-know basis, encryption, and access authorization are all measures that are utilized within the facilities. In addition, the systems that receive the data from DAS are covered entities under the HIPAA Privacy Rules (see 45 CFR Part 160 and Subparts A and E of Part 164). These rules established a national privacy standard for medical records across the healthcare industry including restricting access to the data. By limiting the scope of data exchanges to only HIPAA covered entities, VA can reasonably expect that the receiving system has implemented safeguards to protect the information in compliance with the existing federal regulations.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.
This system processes data from other authoritative sources and does not collect data from the subject/individual of the data. Therefore, notice is provided by the authoritative source and maintained in accordance with this SORN.
System of Record Notice (SORN) Sorn 2021-01516 / 168VA005 Health Information Exchange–VA, https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf
This Privacy Impact Assessment (PIA) also serves as notice of the DAS System. 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 agency, publication in the Federal Register.

6.1b If notice was not provided, explain why.
This system processes data from other authoritative sources and does not collect data from the subject/individual of the data. Therefore, notice is provided by the authoritative source and maintained in accordance with this SORN.

DAS does not collect information directly from the Veteran. The source systems collecting the information would provide notice. In addition, the System of Record Notice (SORN) Sorn 2021-01516 / 168VA005 Health Information Exchange–VA, https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf indicates all purposes of use and records categories stored in the DAS system.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.
This system processes data from other authoritative sources and does not collect data from the subject/individual of the data. Therefore, notice is provided by the authoritative source and maintained in accordance with this SORN.

The System of Record Notice (SORN) Sorn 2021-01516 / 168VA005 Health Information Exchange–VA, https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf indicates all purposes of use and records categories stored in the DAS system.

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.

While DAS does not collect information directly from the Veteran, but instead from the source applications listed in section 1.2 of this PIA, depending on the information required, some data collection is mandatory while others are voluntary. Failure to provide information may result in denial of access to the health care system.

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 system processes data from other authoritative sources and does not collect data from the subject/individual of the data. Therefore, notice is provided by the authoritative source and maintained in accordance with this SORN.

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 to consent to use the information would be handled by the source systems that collect the information from the Veteran and feed DAS with information. The source applications are listed in section 1.2 of this PIA.

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 Privacy Officer (PO) 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: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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: Insufficient notice for consent could result in unapproved use of patient data. Any right to consent to use the information would be handled by the source systems that collect the information from the Veteran and feed DAS with information. The source applications are listed in section 1.2 of this PIA.

Mitigation: The VA mitigates this risk by providing the public with notice that the system exists, as discussed in detail in Question 6.1 under the System of Record Notice.

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals seeking information regarding access to and contesting of records in this system may write the Director, VHIE, Office of Health Informatics/Veterans Health Administration at VACO, 810 Vermont Avenue NW, Washington, DC 20420, or contact their closest VAMC. Requests should contain the full name, address and telephone number of the individual making the inquiry.

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)?

DAS does not collect information directly from the Veteran, but instead from the source applications. Individuals seeking information regarding access to and contesting of records in this system may write the Director, VHIE, Office of Health Informatics/Veterans Health Administration at VACO, 810 Vermont Avenue NW, Washington, DC 20420, or contact their closest VAMC. Requests should contain the full name, address and telephone number of the individual making the inquiry.

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?

Individuals seeking information regarding access to and contesting of records in this system may write the Director, VHIE, Office of Health Informatics/Veterans Health Administration at VACO, 810 Vermont Avenue NW, Washington, DC 20420, or contact their closest VAMC. Requests should contain the full name, address and telephone number of the individual making the inquiry

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.

Individuals wishing to obtain more information about access, redress, and record correction of DAS should contact the Director Standards and Interoperability, Chief Health Informatics office/Office of Health Informatics/Veterans Health Information, Department of Veterans Affairs, 810 Vermont Avenue NW., Washington, DC 20420. Department of Veterans Affairs (VA) ‘‘Sorn 2021-01516 /168VA005 Health Information Exchange-VA”.

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.

Individuals wishing to obtain more information about access, redress, and record correction of DAS should contact the Director Standards and Interoperability, Chief Health Informatics office/Office of Health Informatics/Veterans Health Information, Department of Veterans Affairs, 810 Vermont Avenue NW., Washington, DC 20420. Department of Veterans Affairs (VA) ‘‘Sorn 2021-01516 /168VA005 Health Information Exchange-VA”.

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.

There are no provisions for correcting inaccurate or erroneous information in DAS. The information in DAS is obtained electronically from other systems listed in section 1.2 of this PIA. Instead, they should contact their closest VA Medical Center (VAMC). Inquiries should include the person’s full name, social security number, location and dates of treatment or location and dates of employment, and their return address. Department of Veterans Affairs (VA) ‘‘Sorn 2021-01516 /168VA005 Health Information Exchange-VA.

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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

Mitigation: By publishing this PIA, and the applicable SORN, 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, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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 individuals accessing the DAS system must have a VA background investigation, proper training for their assigned role, and an approved ePAS request.

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?

Outside agencies are not allowed access to the system.

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.

A role-based access control (RBAC) security approach is used to limit users only to the information needed to do their job and prevent them from accessing information that doesn't pertain to them. A variety of user roles, ranging from read-only to operations/administration, will exist in the system.

8.2a. Will VA contractors have access to the system and the PII?

Yes, VA contractors will have access to the system.

8.2b. What involvement will contractors have with the design and maintenance of the system?

VA contractors develop and maintain the DAS system.

8.2c. Does the contractor have a signed confidentiality agreement?

The contractor does not have a confidentiality agreement.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

The contractor does not have a BAA.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?

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.

The contractor only has signed NDAs on an as needed basis for specific pre-procurement sensitive project activities. VA contracts are reviewed determined to the current contract standings. In general, the contract is reviewed per the period of performance as outlined within the documentation and approved by the TAC. Contractors employed for the stated period of performance must pass a MBI, be able to qualify for a Public Trust level clearance that is inclusive of supplying fingerprints and be approved for a Personal Identity Verification card issued by the VA enterprise. Levels of access across the DAS information system team are on a need to know basis with only the necessary level of access required for their specific job requirements only after proper training has been obtained. These trainings are required to be performed annually to maintain their access. Due to the nature of the DAS program being a middleware operation, there are times that team members will need to review file stored or processed by the system for troubleshooting and resolution purposes for both internal and external partners. These files may contain sensitive information inclusive of both PII and PHI.

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

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.
This question is related to privacy control AR-5, Privacy Awareness and Training.
The 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 Talent Management System (TMS). All contractors are cleared using the VA background investigation process and must obtain a Moderate Background Investigation (MBI).
TMS courses that are required:
VA 10176: Privacy and Info Security Awareness and Rules of Behavior
VA 10203: Privacy and HIPAA Training
VA 3812493: Annual Government Ethics Role-based Training
Additional, advanced role-based training maybe required dependent upon the team member roles and responsibilities as defined by the period of performance specifics.
TMS courses for role-based training includes but is not limited to and based on the role of the user.
VA 1016925: Information Assurance for Software Developers IT Software Developers
VA 1357084: Information Security Role-Based Training for Data Managers
VA 64899: Information Security Role-Based Training for IT Project Managers
VA 3197: Information Security Role-Based Training for IT Specialists
VA 1357083: Information Security Role-Based Training for Network Administrators
VA 1357076: Information Security Role-Based Training for System Administrators

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 24 March 2023
3. *The Authorization Status:* ATO
4. *The Authorization Date:* 10 March 2022
5. *The Authorization Termination Date:* 09 March 2025
6. *The Risk Review Completion Date:* 08 March 2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/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. ***(Refer to question 1.8 of the PTA)***

Yes, VAEC Clouds

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)* *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

N/A

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

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

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

N/A

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

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

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

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**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2024.12.02 09:38:00 -07'00'

Privacy Officer, Julie Drake

ERIC ABRAHAM Digitally signed by ERIC ABRAHAM
Date: 2024.12.02 10:55:20 -06'00'

Information System Security Officer, Eric Abraham

JOHN TIRRELL Digitally signed by JOHN TIRRELL
Date: 2024.12.02 12:09:26 -05'00'

Information System Owner, John Tirrell

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:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)