Privacy Impact Assessment for the VA IT System called:

Data Access Services (DAS) Cloud

VA OIT EPMD Enterprise Services PMO
VA OIT

Date PIA submitted for review:

December 16, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita Grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Andre Davis	Andre.Davis2@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?" and will be published online to accompany the PIA link.

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.

DAS is located at the VA Amazon Web Services (AWS) GovCloud facility at 410 Terry Avenue North, Seattle WA 98109. VA AWS GovCloud is a commercial facility owned by Amazon Inc. under contract for services provided to the VA. The VA has issued a FISMA High Authority to Operate (ATO) for the VA AWS GovCloud, which is an isolated AWS region subject to FedRAMP High security controls. All information processed and stored by DAS is fully owned and retained by the VA and DAS.

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?*

- Data Access Services (DAS), VA OIT EPMD Enterprise Services PMO.
- VA Office of Information and Technology.
- System ownership: VA Owned and non-VA Operated.
- 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 grow.
- DAS Cloud 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 partner.
- DAS Cloud 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 Cloud aggregates the response data from multiple Producers to provide to the Consumer.
- The DAS application is physically housed in VA AWS GovCloud, a commercial facility owned by Amazon Inc. under contract for services provided to the VA.
- 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." These guidelines assist in the implementation of these status.
- No current changes to system, only the required 3-year annual review.
- No current technology changes to the system.
- System is not in the process of being modified.
- Sorn 2021-01516 /168VA005 Health Information Exchange-VA.

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)

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>

PII Mapping of Components

DAS Cloud consists of one key component (database). The component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by DAS Cloud and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
DAS Application Service	**YES**	**YES**	**Name, Mailing Address, Zip Code, Phone number, Email, Claim number, Social Security Number, Medical Records, Pharmacy Records**	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).	The minimum-security requirements for DAS cover 17 security-related areas regarding protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media

					protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facilities employ all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives

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.

• Centers for Medicare & Medicaid Services (CMS) – This is a bidirectional service with VA to determine health coverage/eligibility.

• Veteran's Benefits Management System (VBMS) – DAS receives subscription requests from VBMS to identify and retrieve documents that facilitate claims adjudication.

• Non-VA Clinicians – DAS accepts and stores secure health information from non-VA providers through eHealth Exchange partners and contracted vendors.

• VBMS & VBA – VBMS and VBA work with DAS to provide storage, transport, and validation of exam requests and Disability Benefits Questionnaires (DBQs).

• Clinical User Interface (CUI) – VHA clinicians will use the CUI to identify the findings of a Disability Assessment Exam in order to assist VBA to adjudicate claims.

• Department of Defense (DoD) Personal Medical Coordinator (PMC) – 180 days before a service member separates, a Pre-Separation Rating can be established to speed up eBenefits upon separation.

• Department of Defense (DoD) – DAS accepts the first 17 documents comprising the Electronic case file (eCFT) from DoD that VA requires to begin the Integrated Disability Evaluation System (IDES) process. Partners are Guard Bureau and VBMS.

• Social Security Administration (SSA)/eHealth Exchange – SSA through eHealth Exchange sends Opt-In Forms. Forms are stored in Veterans Authorizations and Preferences Enhanced system (VAPE).

• Department of Defense (DoD) Care Coordinators Program – This is a bidirectional exchange between DoD and VA Care Coordinators Profiles.

• Veterans Administration (VA)/ Veterans Relationship Management (VRM)/ Veterans Benefits Administration (VBA) – These organizations transport claims data to Eligibility Record Services (VIERS) for the purpose of processing claims.

• eHealth Exchange, Walgreens – DAS transports Veterans' immunization data to VistA sites. Partners include VLER Health, Walgreens, and Immunizations.

• Veteran Reentry Search Service (VRSS) – DAS transports files between Correctional Facilities and Court Systems, and the VRSS web application, so that the facilities can identify Veterans within their institution's population.

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.

- CMS – CMS sends queries through the DAS Proxy Service to VIERS. After receiving the query, VIERS then communicates a Veterans' Affordable Care Act (ACA) eligibility to DAS, which then communicates this information to CMS.
- VBMS – VBMS sends DAS a subscription request to obtain Veteran data from Healthcare Artifact and Image Management Solution HAIMS.
- Non-VA Clinicians – Clinicians send DAS individual Veterans' secure health information on in the format of C32.
- VBMS & VBA – VBMS opens a claim request Disability Exam in Disability Exam and Assessment Program DEAP. DEAP then sends the exam request to DAS, at which point DAS sends the request to VBA.
- Clinical User Interface (CUI) – AVHA Clinician will use the CUI to identify the findings of a Disability Assessment Exam via xml data that DAS sends to the VBMS calculator.
- Department of Defense (DoD) Personal Medical Coordinator (PMC) – The primary source of information is the DBQ that's completed by a Veteran. Once the Veteran has filled out the DBQ, DAS notifies VBMS. VBMS then performs a rating, which is sent back to DoD.
- National Guard Bureau – DoD sends eCFT documents to DAS to store for access by VBMS so that DoD and VBA can determine the disability rating of the Service Member.
- Social Security Administration (SSA)/eHealth Exchange – DAS writes forms from SSA to Veterans Authorizations and Preferences (VAP). SSA then requests an Electronic Health Record (EHR) for the Veteran through eHealth Exchange. SSA through eHealth Exchange then sends an Op-In Form.
- Airborne Hazards Open Burn Pit Registry (AHOBPR) – The primary source of information is through Veterans' self-entered questionnaires.
- Care Coordinators Program – Data is retrieved from a query based on a Veteran's name or other indexed file.
- Veterans Administration (VA)/ Veterans Relationship Management (VRM)/ Veterans Benefits Administration (VBA) – Digits-to-Digits (D2D) obtains information on D2D claims through use of VIERS through DAS proxy services.
- eHealth Exchange – VLER Health, Walgreens, and Immunizations send data to DAS, and DAS then sends that immunization data to VistA sites.
- Veteran Reentry Search Service (Pilot Completed) (VRSS) – Facilities provide comma separated values CSV file to VRSS, that then interfaces with the Veterans Affairs/Department of Defense Information Repository (VADIR), which uses an automated algorithm to identify individuals from the file who have served in the military.
- Centralized Administrative Accounting Transaction System (CAATS) – VBMS sends a request for a C&P exam to DAS. DAS stores the request and then sends it to an external, VVA-contracted examiner.

- Care in the Community – DAS stores and shares all third-party data from the Care in the Community Initiative. This will include data from medical treatment, payment of claims, and insurance.

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.

Some of the information is imported 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 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.

1.5 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

SSN serves as the Medical Record Number and Unique Identifier for the Veteran. Legal Authority: 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." These guidelines assist in the implementation of these statutes.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: DAS Cloud collects Personally Identifiable Information (PII) and other highly delicate protected health information (PHI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and /or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties so that they may find the help they need to get through their crisis. DAS Cloud employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These security measures include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security;

risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Section 2. Uses of the Information

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

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

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

- Name - Veteran's identification.
- Mailing Address - Used to correspond with the Veteran as well as confirm Veteran's identity.
- Zip Code - Part of the mailing address.
- Phone Number - Used to correspond with the Veteran as well as confirm Veteran's identity.
- Email - Used to correspond with the Veteran as well as confirm Veteran's identity.
- Claim number - Used to confirm Veteran's identity.
- Social Security Number - Used to verify Veteran's identity.
- Veteran 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.
- Pharmacy Records - To check the type of medication used by patients.

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

- DAS Cloud 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 serves two main purposes:

- Bidirectional Exchange of structured and unstructured information within the VA and other provider partners.

- Correlation of patient identities between VA and other provider partners including the Department of Defense (DoD).

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

All data and SSNs are encrypted during transit and at rest.

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

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

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

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

The minimum-security requirements for DAS Cloud high impact system cover 17 security-related areas regarding protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facilities employ all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans' information is used, stored, and protected.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system.
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

- Name, Social Security Number, Mailing address with Zip Code, Phone number.
- Email address, Medical Records, Pharmacy Records, Claim number.

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.

In accordance with the records disposition authority approved by the Archivist of the United States, health information stored on electronic media storage is permanently transferred to the National Archives after the last episode of patient care.

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.

These records are retained in accordance with the General Records Schedule Sections 3.0 Technology and 4.0 Information Management, approved by National Archives and Records Administration (NARA) http://www.archives.gov/records-mgmt/grs.html.

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

Records/digital information will be eliminated following the sanitization procedures in VA Handbook 6300.1 Records Management Procedures and VA Handbook 6500.1 Electronic Media Sanitization. Schedule 3.0 and 4.0, approved by National Archives and Records Administration (NARA).

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

DAS Cloud system only utilizes test data for testing purposes. All test data has been approved by the Privacy Office prior to use.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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:
<u>Privacy Risk:</u> There is a risk that the information maintained by DAS Cloud 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.

<u>Mitigation:</u> To mitigate the risk posed by information retention, DAS Cloud 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.

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VBA VBMS – Disability Benefit Questionnaire (DBQ), Service Treatment Record (STR), and Exam Management	VBMS and VBA work with DAS Cloud to provide storage, transport, and validation of exam requests and Disability Benefits Questionnaires (DBQs) and Service Treatment Records (STRs).	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	TIC Gateway HTTPS using SSL encryption and Certificate exchange.
Compensation and Pension Record (CAPRI) VBA-DBQ	CAPRI, VBMS and VBA work with DAS Cloud to provide storage, transport, and validation of exam requests and Disability Benefits Questionnaires (DBQs).	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	HTTPS using SSL encryption and Certificate exchange.

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***
Veteran Information/ Eligibility Reporting System (VIERS) VBA- Digits 2 Digits (D2D)	DAS Cloud transports data to VIERS to determine a Veteran's eligibility status and ACA status.	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	HTTPS using SSL encryption and Certificate exchange.
VHA - Direct Secure Messaging (DSM)	Secure email portal with external providers that stores attachments in DAS Cloud.	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	HTTPS using SSL encryption and Certificate exchange.
VHA - Legacy Viewer Sustainment (LVS)	DAS Cloud transports DoD data to LVS for clinical use.	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	HTTPS using SSL encryption and Certificate exchange.
VHA - Joint Legacy Viewer (JLV)	DAS Cloud transports eHX provider data to JLV for clinical use.	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	HTTPS using SSL encryption and Certificate exchange.
VHA - Central VistA Image Exchange (CVIX)	Bi-Directional exchange with DoD for Veteran health data.	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	HTTPS using SSL encryption and Certificate exchange.
VHA - Veteran Re-Entry Search Service (VRSS)	DAS Cloud sends a CSV file provided by external facilities to determine if an individual has served in the military.	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	HTTPS using SSL encryption and Certificate exchange.
VHA - Veteran Hhealth Information System and Technology Architecture (VistA)	For Veterans' immunization data.	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	HTTPS using SSL encryption and Certificate exchange.
VHA – VistA Integration Adapter (VIA)	Application used to connect/write data to VistA.	Personally Identifiable Information (PII), Protected Health Information (PHI),	HTTPS using SSL encryption and

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***
		and Individually Identifiable Information (III).	Certificate exchange.
VHA - Enrollment Systems Community Care (ESCC)	Sends Veteran eEligibility and demographic information to community care contract vendors for purpose of clinical care.	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	HTTPS using SSL encryption and Certificate exchange.
Veterans Data Integration and Federation (VDIF)	Prescription drug monitoring program reporting data.	No PII or PHI, only statistics.	HTTPS using SSL encryption and Certificate exchange.
VistA ePrescribing (eRx)	Submission of prescriptions with external VHA-contracted vendors.	Personally Identifiable Information (PII), Protected Health Information (PHI).	HTTPS using SSL encryption and Certificate exchange.
Federal Case Management Tool (FCMT)	Sharing of interagency comprehensive continued care plans with DoD for continued care of veterans.	Personally Identifiable Information (PII), Protected Health Information (PHI).	HTTPS using SSL encryption and Certificate exchange.
VA Identity and Access Management (IAM)	Used for patient ID correlation and integrated login.	Personally Identifiable Information (PII). Individually Identifiable Information (III).	HTTPS using SSL encryption and Certificate exchange.
National Precision Oncology Program (NPOP)	Oncology documents and image retrieval submitted by external vendors.	Personally Identifiable Information (PII), Protected Health Information (PHI).	HTTPS using SSL encryption and Certificate exchange.
Provider Profile Management System (PPMS)	Provider profile information for VA providers to support scheduling and network management functions.	Individually Identifiable Information (III).	HTTPS using SSL encryption and Certificate exchange.
Community Care Referrals and Authorizations (CCRA)	Referrals, authorizations, and storage of community care related data.	Personally Identifiable Information (PII), Protected Health Information (PHI).	HTTPS using SSL encryption and Certificate exchange.
Enterprise Program Reporting System (EPRS)	Reporting capabilities for community care data submitted by external vendors.	Personally Identifiable Information (PII), Protected Health Information (PHI).	HTTPS using SSL encryption and Certificate exchange.

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***
Community Care Reimbursement System (CCRS)	Submission of NCPDP files for community administered care.	Personally Identifiable Information (PII), Protected Health Information (PHI).	HTTPS using SSL encryption and Certificate exchange.
Signature Informed Consent (SIC)	Routing of patient consent documents for care.	Personally Identifiable Information (PII), Protected Health Information (PHI).	HTTPS using SSL encryption and Certificate exchange.
Telecare Record Manager (TRM)	Routing of telecare records between Cerner and VA clinicians.	Personally Identifiable Information (PII), Protected Health Information (PHI).	HTTPS using SSL encryption and Certificate exchange.
Dental Record Manager (DRM)	Routing of dental records between VA and Cerner clinicians.	Personally Identifiable Information (PII), Protected Health Information (PHI).	HTTPS using SSL encryption and Certificate exchange.
Beneficiary Travel Self Service System (BTSSS)	Routing of self-service travel data.	Personally Identifiable Information (PII), Protected Health Information (PHI).	HTTPS using SSL encryption and Certificate exchange.
InteleRad	Routing of appointments and medical order messages between Cerner and VA site InteleRad PACS.	Personally Identifiable Information (PII), Protected Health Information (PHI).	HTTPS using SSL encryption and Certificate exchange.
TeleICU	Routing of clinical data and notes for TeleICU consults.	Personally Identifiable Information (PII), Protected Health Information (PHI).	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 Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The privacy risk 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 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***
Logistics Health Incorporated (LHI)	LHI provides medical disability examinations for Veterans. The LHI will provide a protected electronic environment to receive VA case referrals and distribute final examination reports.	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) – Secure Socket Layer – Virtual Private Network (SSL – VPN).
Quality, Timeliness, Customer Service Management, Inc. (QTC)	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.	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) – Secure Socket Layer – Virtual Private Network (SSL – VPN).
Veterans Evaluation Services (VES)	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	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) – Secure Socket Layer – Virtual Private Network (SSL – VPN).

	electronically transferred to the VA.			
Vetra Spec System	DataSpec, Inc. provides software as a Claims Management System to Veteran's Service Organizations (VSO's).	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) –Secure Socket Layer – Virtual Private Network (SSL – VPN).
Bene Vets	Bene Vets provides software as a Claims Management System to Veteran Service Organizations (VSO's).	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) –Secure Socket Layer – Virtual Private Network (SSL – VPN).
The Change Healthcare ePrescribing (eRx).	Verifies and transmits eRx transactions to/from external provider (Electronic Health Record) EHR systems and the VA Infrastructure, i.e., DAS system.	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) –Secure Socket Layer – Virtual Private Network (SSL – VPN).
HAIMS (Healthcare Artifacts and Image Management System)	DoD system with which DAS sends and receives Veteran health data/artifacts.	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) –Secure Socket Layer – Virtual Private Network (SSL – VPN) Federal Information Processing Standard (FIPS) 199.
DMIX Exchange Service / Department of Defense (DoD)	DoD system with which DAS sends and receives Veteran health data/artifacts.	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) –Secure Socket Layer – Virtual Private Network (SSL – VPN) Federal Information Processing Standard (FIPS) 199.
Tri-West System	Tri-West provides software as a Claims Management System	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) – Secure Socket Layer – Virtual Private Network (SSL – VPN)

	to Veteran Service Organizations (VSO's).			Federal Information Processing Standard (FIPS) 199.
Centers for Medicare and Medicaid Services (CMS)	This is a bidirectional service with VA to determine health coverage/eligibility.	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) – Secure Socket Layer – Virtual Private Network (SSL – VPN) Federal Information Processing Standard (FIPS) 199.
Foundation Medicine Inc (FMI) System	Oncology documents and image submission to VA.	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) – Secure Socket Layer – Virtual Private Network (SSL – VPN) Federal Information Processing Standard (FIPS) 199.
Interqual Inc System	Generic medical procedure data to determine treatment plans.	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) – Secure Socket Layer – Virtual Private Network (SSL – VPN) Federal Information Processing Standard (FIPS) 199.
DoD Case Management System (DoD CMS)	Sharing of interagency comprehensive continued care plans with VA for continued care of veterans.	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) – Secure Socket Layer – Virtual Private Network (SSL – VPN) Federal Information Processing Standard (FIPS) 199.
Cerner Federal Enclave (OpenLink, Rhapsody, FHIR Ignite, Citrix, LILA)	Exchange of data for veteran care and benefits.	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) – Secure Socket Layer – Virtual Private Network (SSL – VPN) Federal Information Processing Standard (FIPS) 199

Life Image Inc System	DICOM images for patient care.	PII/PHI	ISA/MOU	Hypertext Transfer Protocol (HTTPS) – Secure Socket Layer – Virtual Private Network (SSL – VPN) Federal Information Processing Standard (FIPS) 199

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:
Privacy Risk: The privacy risk associated with maintaining PII is that sharing data outside of the Department of Veteran's Affairs could 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 Cloud 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 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.

System of Record Notice (SORN) Sorn 2021-01516 /168VA005 Health Information Exchange-VA. https://www.oprm.va.gov/docs/Current_SORN_List_12_3_2021.pdf

This Privacy Impact Assessment (PIA) also serves as notice of the DAS Cloud 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.

6.2 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 Cloud 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 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 Cloud with information. The source applications are listed in section 1.2 of this PIA.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Follow the format below:
Privacy Risk: 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 Cloud 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 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.

Individuals wishing to obtain more information about access, redress, and record correction of DAS Cloud 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.

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 Cloud 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 who wish to determine whether this system of records contains information about them 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".

7.4 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 DAS Cloud. The information in DAS Cloud 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.*

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

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

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

Follow the format below:
Privacy Risk: There is a risk that 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.

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.

1. Access to and use of national administrative databases, warehouses, and data marts is limited to those persons whose official duties require such access, and the VA has established security procedures to ensure that access is appropriately limited. Information security officers and system data stewards review and authorize data access requests. VA regulates data access with security software that authenticates users and requires individually unique codes and passwords. VA provides information security training to all staff and instructs staff on the responsibility each person has for safeguarding data confidentiality.

2. Physical access to computer rooms housing national administrative databases, warehouses, and data marts is restricted to authorized staff and protected by a variety of security devices. Unauthorized employees, contractors, and other staff are not allowed in computer rooms. The Federal Protective Service or other security personnel provide physical security for the buildings housing computer rooms and data centers.

3. Data transmissions between operational systems and national administrative databases, warehouses, and data marts maintained by this system of record are protected by state-of-the-art telecommunication software and hardware. This may include firewalls, intrusion detection devices, encryption, and other security measures necessary to safeguard data as it travels across the VA Network.

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.

Yes, contractors will have access to the system. Contracts are reviewed annually at a minimum by the VA Contractor Officer Representative (COR) and the VA Project Manager (PM). 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).

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.

Users are required to complete information system security and privacy training activities including annual security awareness training and specific information system security training. The training records are retained for 7 years. This documentation and monitoring process is performed using the Talent Management System (TMS).

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.***

Yes, completed Stage 4 Control Assessment moved to Stage 5 Authorization, Authorization termination 10 April 2022, Risk assessment completed 29 September 2019, FIPS Classification 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.

Yes, VAEC GovCloud

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.

VA owns this contract, not DAS, but VA maintains ownership of all data.

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.

No, CSP does not collect any ancillary data.

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 - Cloud Provider (AWS) does not hold any privacy data on behalf of DAS. VA is held responsible for the security and privacy of DAS.

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).

No.

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: 2021.12.29 13:16:45 -05'00'

Privacy Officer, Rita Grewal

Andre L. Davis 1130018

Digitally signed by Andre L. Davis 1130018
Date: 2021.12.29 08:27:50 -06'00'

Information Systems Security Officer, Andre Davis

John Tirrell 304978

Digitally signed by John Tirrell 304978
Date: 2022.01.03 09:39:45 -05'00'

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).

System of Record Notice (SORN) Sorn 2021-01516 /168VA005 Health Information Exchange-VA.

https://www.oprm.va.gov/docs/Current_SORN_List_12_3_2021.pdf