SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements
under the Federal Information Security Management Act (FISMA).

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

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

Disability and Medical Assessment (DMA) Quality Audit Tool (QAT)

Office of Disability and Medical Assessment (DMA)

Date PIA submitted for review:

May 18, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Takeshia Berkeley	Takeshia.Berkeley@va.gov	404-828-5337
Information System Security Officer (ISSO)	Howard Knight	Howard.Knight@va.gov	404-828-5340
Information System Owner	Louise Rodebush	Louise.Rodebush@va.gov	216-849-0193

Abstract

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

The Quality Audit Tool (QAT) is used to audit the compliance and completeness of the Compensation and Pension (C&P) Disability Examination reports. A random sampling of the C&P Exam reports are audited against specific criteria to help determine whether the reports are correct and complete enough for VA's disability determination adjudication purposes.

Overview

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

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

The Disability and Medical Assessment (DMA) Quality Audit Tool (QAT) is an information system under the responsibility of Office of Disability and Medical Assessment. The Veterans Health Administration's (VHA) DMA Quality Department conducts focused ratability reviews of compensation and pension (C&P) disability examination requests and reports using the QAT. The review process allows for a substantive review performed against any disability examination, whether performed by a VHA clinician or fee-for service clinician, who utilizes CAPRI, or a VHA contracted clinician. DMA's Quality Team is committed to providing examination report reviews in a fair and accurate manner. In order to promote performance improvement, an appeal process has been established to allow for a second review of disputed audit scores.

The QAT is used to audit the compliance and completeness of the Compensation and Pension (C&P) Disability Examination requests and reports. A random sampling of the C&P Exam requests and reports are audited against specific criteria to help determine whether the reports are correct and complete enough for adjudication purposes.
The DMA QAT is not a regional GSS, VistA, or LAN. There is no information sharing performed this information system. DMA QAT is only hosted at one location, the HEC. It operates under the legal authority of:

- 38 U.S. Code § 5103A - Duty to assist claimants
- 38 CFR 3.159 - Department of Veterans Affairs assistance in developing claims
- 38 CFR 3.326 – Examinations

No technology change is expected upon completion of this PIA. No SORN amendment or revision required. System does not use cloud technology.
The magnitude of potential harm if privacy related data is disclosed is high, due to the potential for identity theft. The reputation of both the DMA and VA could be negatively impacted by a privacy related data disclosure.

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)

The tool maintains the exam 2507 request for the claimant, which contains protected health information (PHI). We maintain in the database the name of the clinical provider that is conducting the examination as well as their social security number (SSN).

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

PII Mapping of Components

The Disability and Medical Assessment (DMA) Quality Audit Tool (QAT) consists of one key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by DMA 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. The first table of 3.9 in the PTA should be used to answer this question.

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
dbCPEP	Yes	Yes	Patient and Clinician Names, Patient and	Evaluation of clinician training and performance for DMA	SSL, and database encryption

			Clinician SSNs, Exam info.	**exams, and reporting.**	
CDWWork	**Yes**	**Yes**	Social Security Number, Exam Type	**This is the VA wide Data Warehouse repository.**	**SSL, and database encryption**
DMA_Quality	**Yes**	**Yes**	Social Security Number, Exam Type	**For performance review of facilities performing DMA examinations.**	**SSL, and database encryption**
DMA_CP_Registration_Certification	**Yes**	**Yes**	Social Security Number	**Clinician identify verification and certification to perform the DMA examinations.**	**SSL, and database encryption**

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.

The data underlying the C&P process is created by C&P practitioners using the Disability and Medical Assessment (DMA) Compensation and Pension Record Interchange (CAPRI) application and stored in the local Veterans Health Information Systems and Technology Architecture (VistA) databases at each VA Medical Center (VAMC) across the country. The Veterans Health Administration (VHA) Corporate Data Warehouse (CDW) collects the C&P data stored in 130 VistA databases nationwide and stores the aggregate data in a central data

repository. The Quality Audit Tool extracts data once per month from the Corporate Data Warehouse to allow review of C&P Disability Exam reports. A connection is made with the Clinician Registration and Certification Tool to verify whether or not the clinician performing the exam was certified and credentialed for the type of exam.

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.

Data is collected via a database Extract Transform and Load (ETL) process using SQL Server Integration Services (SSIS), and stored procedures in Structured Query Language SQL Server.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The reviewer cross-checks information with CAPRI and Veterans Benefits Management System (VBMS) each time a quality review is completed.

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

In order to evaluate the quality of the examination reports, it is necessary to pull from the Corporate Data Warehouse the exact examination reports received. These are collected by VHA and Veterans Benefits Administration (VBA) by SSN. Authority: 38 U.S.C. 5103A, and 38 CFR 3.159 and 3.326.

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: This table describes the information system categorization. For an information system, the respective security objectives (confidentiality, integrity, availability) shall be the highest security categories that have been determined for each type of information that:

Confidentiality	High
Integrity	Moderate
Availability	Moderate
Security Category (SC)	High

Mitigation: The Quality tool is only viewable on the VA network. Quality Team business users are screened by the Quality Team Manager and trained prior to access being granted. Authorized users are required to sign the National Rules of Behavior (or Contractor Rules of Behavior) as part of the annual Privacy and Security Awareness training, which is documented in the VA Talent Management System (TMS).

Section 2. Uses of the Information

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

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

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

The Quality tool allows Quality Reviewers access to statistically valid random sampling that cannot be accomplished via any other applications or tools within Veterans Affairs (VA).

2.2 What types of tools are used to analyze data and what type of data may be produced?

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The data produced by the Quality Audit Tool is used for performance assessment and business process improvement. For performance assessment, the goal is for all Veterans Integrated Service Networks (VISNs) to achieve a quality score of at least 90% and the data produced by the Quality Audit Tool is used to assess the achievement of this goal quarterly. For business process improvement, the detail data is studied to identify common quality problems that can be improved via targeted training.

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?

In transit information is protected by HTTPS (SSL), and at rest the data in the database is encrypted.

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

Yes, access to view SSNs are only viewable by the high-level administrators, and the team of DMA Quality Reviewers.

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

Access to the database is only granted after staff have completed Privacy training, Cyber Security Training, and signed the Rules of Behavior.

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

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

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

Add answer here:

The Quality tool program does not allow access to any individuals that are not part of the DMA Quality team. Administrative controls are in use that allows only the Administrator to add or remove users from the system. In order to gain access, training is provided by the DMA Quality staff before system access can be granted. When a team member leaves the division, access is removed as part of the check-out process.

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

Veteran/Claimant Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Current Medications, Previous Medical Records, 2507 (VA Disability Examination) request for the Claimant, which may contain manually entered PHI and PII, Clinical Provider Name that completed the 2507 request, and Clinical Provider SSN that completed the 2507 request.

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.

CDW archives both application server and database server audit logs. Per National Archives and Records Administration (NARA) standards, audit logs are retained for 6 years.

CDW data is retained until the CDW Governance Board approves a policy for records disposition. Records Schedule Number DAA-0015-2015-0004 was approved by the National Archives and Records Administration (NARA) and published on 7/13/2015. The aforementioned records schedule has various retention lengths for data types within CDW. Once the CDW Governance Board approves, records will be retained in accordance with the new records schedule.

The records schedule can be found at GRS 3.1 (archives.gov).

The Quality Tool database contains all data gathering elements previously defined and the information needs to be maintained indefinitely. Quality Tool Administrators and the Quality Tool Database Administrator are the only ones that have access to all data. Quality reviewers only see the specific info that is required to complete their necessary reviews on a monthly basis.

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.

Documentation is available on CDW SharePoint site https://vaww.cdw.va.gov/bisl/allbislstaff/SitePages/Home.aspx. Records Schedule Number 3.1 was approved by the National Archives and Records Administration (NARA) and published in January 2017. The records schedule can be found at GRS 3.1 (archives.gov).

3.4 What are the procedures for the elimination of SPI?

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

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA Handbook 6500.1 Electronic Media Sanitization. Austin Information Technology Center (AITC) has an exception memorandum, dated 13 Apr 2015, allowing the center to locally destroy media. The memorandum lists specific methods of sanitization which are approved methods in accordance with VA 6500.1.

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. 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

No. During testing and training, DMA QAT development servers are used. Those servers utilize fictitious information for testing and training purposes.

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:

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

Mitigation: To mitigate the risk posed by information retention, CDW adheres to the Records Schedule approved by NARA. When the retention date is reached for a record, the data is carefully disposed of by the approved method as described in Records Schedule in accordance with VA 6500.1 HB media and destruction policies. Records Schedule Number 3.1 was approved by the National Archives and Records Administration (NARA) and published in January 2017.

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***
VHA Support Service Center	Those with access can review results	Veteran's name and SS#, examiners name, exam type	SQL Server Management Studio ETL job
SHared REporting Database (SHRED)	Those with access can review results	No personal identifiable information (PII) stored	Manual data push between SQL Server databases
VBA, VISN and facility point of contact (POCs)	To improve quality requests and reports	Veteran's name and SS#, examiners name, exam type	Manual data pull by running VSSC quality report

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: There is a risk that data contained in the CDW may be shared with unauthorized individuals or that authorized individuals may share it with other unauthorized individuals. Examples of this risk would be an unauthorized person breeched the system or a VA sponsored user shares data outside of the VA boundary without express written permission.

Mitigation: The Quality tool is only viewable on the VA network. Quality Team business users are screened by the Quality Team Manager and trained prior to access being granted. Authorized users are required to sign the National Rules of Behavior (or Contractor Rules of Behavior) as part of the annual Privacy and Security Awareness training, which is documented in the VA Talent Management System (TMS).

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***
N/A	N/A	N/A	N/A	N/A

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: N/A: Data from the Quality tool is not shared outside of the Veterans Affairs (VA).

Mitigation: N/A: Data from the Quality tool is not shared outside of the Veterans Affairs (VA).

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

CDW does not use personal information for secondary purposes. The VA provides notice of intended uses of PII/PHI collected from individuals through the VA privacy policy. The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A signed statement acknowledging that the individual read and understood the NOPP is scanned into each applicant's electronic file. When updates are made to the NOPP copies are mailed to all VHA beneficiaries. In addition, when the VA collects personal data from an individual, the VA will inform individuals of the intended uses of the data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act system notice has been published in the Federal Register and posted on the VA Systems of Records Notices (SORN) 172VA10P2, 121VA10P2, and 79VA19 When routine and established uses of PII/PHI change, the VA will amend SORNs and publish notification of amendment in the Federal Register to notify individuals of new and intended uses of PII. DMA QAT is a tool used by DMA SMEs.

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

The VA provides notice of intended uses of PII/PHI collected from individuals through the VA privacy policy. In addition, when the VA collects personal data from an individual, the VA will inform individuals of the intended uses of the data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act system notice has been published in the Federal Register and posted on the VA Systems of Records Notices 172VA10P2, 121VA10P2, and 79VA19. When routine and established uses of PII/PHI change, the VA will amend SORNs and publish notification of amendment in the Federal Register to notify individuals of new and intended uses of PII.

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually-identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

The CDW system receives the bulk of source data from the VISTA system; therefore, notice of the right of refusal would be addressed by source system. Notice and Right to Decline are provided by research protocols supplying information to the CDW system.
A Privacy Act Notice is provided to active participants of VA research studies. If a participant in a research study declines to provide information the participant may not be eligible to continue to participate in the research study. In accordance with VHA Handbook 1200.05, a written HIPAA authorization signed by the individual to whom the information or record pertains is required when VA health care facilities need to utilize individually-identifiable health information for a purpose other than treatment, payment, or health care operations (e.g., research) (VHA Handbook 1605.1).

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

The VA provides notice of intended uses of PII/PHI collected from individuals through the VA privacy policy. In addition, when the VA collects personal data from an individual, the VA will inform individuals of the intended uses of the data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act system notice has been published in the Federal Register and posted on the VA Systems of Records Notices (SORN). When routine and established uses of PII/PHI change, the VA will amend SORNs and publish notification of amendment in the Federal Register to notify individuals of new and intended uses of PII.

While individuals may have the ability to consent to various uses of their information at the VA, they do not have the ability to consent or deny the use of their information as part of the CDW & Quality Tool systems due to CDW getting most of its data from VISTA. Right to consent would be determined by the source system.

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

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

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

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

Follow the format below:
Privacy Risk: There is a risk that members of the public may not know that the CDW system exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk of not providing notice to the public as discussed in detail in question 6.1 above, the PIA and SORN 172VA10P2, 121VA10P2, 79VA19 are published to notify and inform the public that information collected by the VA is stored in the CDW system. Active participants in research studies are given notice and informed consent documents prior to their information being collected for the study.

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.

The VA Privacy Service monitors and documents any anomalies or problems to improve the Privacy controls. This control is the responsibility of the VA.

The VA provides notice of intended uses of PII/PHI collected from Claimants/Veterans through the VA privacy policy. In addition, when the VA collects personal data from an individual, the VA will inform individuals of the intended uses of the data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act system notice has been published in the Federal Register and posted on the VA Systems of Records Notices (SORN). When routine and established uses of PII/PHI change, the VA will amend SORNs and publish notification of amendment in the Federal Register to notify individuals of new and intended uses of PII.

Individuals wishing to obtain more information about access, redress and record correction of CDW system should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) 121VA19 - National Patient Databases-VA. This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2004-04-07/pdf/04-7821.pdf

For DMA's Quality Tool:
VHA Clinics access quality review data results via VSSC as described in 4.1.
Usage of the DMQ Quality tool is limited to DMA Quality Reviewers and Administrators.

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.

Corrections (Appeals) are requested by VHA Compensation & Pension (C&P) Clinics via secure email. The original DMA Quality Reviewer analyzes the appeal request and makes a validity determination. A second quality review specialist analyzes the appeal request, the first reviewer's comment, and makes a validity determination. The appeal is then sent to the Quality Team Manager, who renders a final determination. The final determination is sent via secure email to the clinic requesting the appeal.
If the appeal is granted and a change to the database is needed, a ticket is submitted to the National Service Desk (NSD), which is passed onto the Quality Tool database admin for correction.

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.

Procedures for the DMA Quality review process and subsequent appeals can be located within DMA's website at the following locations:
http://vaww.dma.va.gov/index.asp
http://vaww.dma.va.gov/quality_resources.asp
http://vaww.dma.va.gov/cp_publications.asp

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.

Not applicable, formal redress is provided as stated above in section 7.3.

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: This section is not applicable to CDW or the DMA Quality Tool. Individuals do not access their records though this system, so the risk is low.

Mitigation: This section is not applicable to CDW or the DMA Quality Tool. Individuals do not access their records though this system, so the risk is low.

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.

The Quality tool is only viewable on the VA network. Quality Team business users are screened by the Quality Team Manager and trained prior to access being granted. Authorized users are required to sign the National Rules of Behavior (or Contractor Rules of Behavior) as part of the annual Privacy and Security Awareness training, which is documented in the VA Talent Management System (TMS).

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 the system developer /database administrator is a VA contractor.

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.

Authorized users are required to sign the National Rules of Behavior (or Contractor Rules of Behavior) as part of the annual Privacy and Security Awareness training, which is documented in the VA 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.***

DMA QAT is currently covered under the Region 6 General Support System (GSS) 120-day Authority to Operate (ATO) signed January 8, 2018 by the Deputy Assistant Secretary IT Operations and Services, Susan McHugh-Polley. This ATO expires on May 8, 2018.

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.

No, no cloud resources are being used at this time. N/A.

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

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

N/A

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

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

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

N/A

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

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

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

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

TAKESHIA BERKELEY

Digitally signed by TAKESHIA BERKELEY
Date: 2022.06.03 10:34:22 -04'00'

Privacy Officer, Takeshia Berkeley

Howard Knight 1508786

Digitally signed by Howard Knight 1508786
Date: 2022.06.01 19:17:17 -04'00'

Information Systems Security Officer, Howard Knight

Louise Rodebush 296012

Digitally signed by Louise Rodebush 296012
Date: 2022.05.31 13:07:53 -04'00'

Information System Owner, Louise Rodebush

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).