Privacy Impact Assessment for the VA IT System called:

Diffusion Marketplace

VHA

Date PIA submitted for review:

06/04/2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Andrea Wilson	Andrea.Wilson3@va.gov	321-205-4305
Information System Security Officer (ISSO)	Merle Kelley	Merle.kelley@va.gov	319-430-7098
Information System Owner	Stefan Test	Stefan.test@va.gov	850-293-0858

Abstract

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

The DMVA is an application hosted on the VAEC AWS GovCloud that's purpose is to share and spread proven innovative healthcare practices across the Veteran's Health Administration (VHA) to become a better learning healthcare system. Practice partners can create practice pages that are a description of an innovative medical or management practice designed to give enough information for potential users to select and implement that practice. Lead others in the discovery of proven, innovative practices and provide resources for implementation. The Diffusion Marketplace portal will be utilized by VA employees within the VA Enterprise via the VAEC (VA Enterprise Cloud).

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.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *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?*
- *Does the system use cloud technology? 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.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*

- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

The owner of Diffusion Marketplace VA (DMVA) is the Veterans Health Administration (VHA). DMVA is the VA's centralized repository for best practices in one marketplace system, and supports the agency by providing an innovative solution to disseminate best practices across the VA. DMVA will be developed and hosted in the Veteran Affairs Enterprise Cloud (VAEC) in accordance with the Cloud and VAEC First Initiatives. The VAEC is currently FedRAMP approved to support moderate and high services. The AWS FedRAMP high AWS RDS PostgreSQL (Relational Database) where all of the information is stored establishes the VA's ownership rights over system data that may include PII such as full name. DMVA is built with practice pages that are a summary description of an innovative medical or management practice designed to give readers (users) enough information to select and implement the practice. The purpose of practice pages is to allow users to find colleagues and subject matter experts to assist in implementing proven best practices. The number of users that we anticipate on our October go live date is 1,000+ users, all of whom will populate personal profiles which contain PII, limited to full name, VA email, job title, general job role, and place of employment. The DMVA user information is encrypted at rest.

In addition, the system will be moderated by users and administrators to report violations of the terms and conditions available in Attachment A. Users are notified of the rules of behavior by the DMVA terms and conditions, which must be read and accepted before registering for the site. Content that is reported as a violation of the Terms of Use is temporarily hidden from the site while it is reviewed by the community management team, and either permanently removed after the content is confirmed to be inappropriate or returned to the site if the content is appropriate. Reports of content violating the Terms of Use are encrypted at rest.

The site is opt-in, and users are VA staff and contractors with Network Accounts across all VA sites. Access, data storage, collection, and retention, and all other aspects of the system are uniform across all sites. PII stored in the system is not shared with organizations within or outside the VA.

The magnitude of harm if privacy related data is disclosed is low. Though PII is stored in the system, most of the PII is publicly released by OPM for VA employees. DMVA will be adopting the PIV multi-factor authentication (MFA) to be integrated into the registration and user sign-in process. Users are warned of the potential risk of disclosing SPI within the system. Additionally, individuals' use of the system is optional, and users can correct or remove their PII at any time or delete their account and opt-out of the system at any time.

Public users will be limited to practices pages that have opted to be shared external to the VA and will require a PIV card to connect to practices pages located behind the firewall.

DMVA is maintained under Veterans' Benefits, Chapter 3: Secretary of Veterans Affairs, Title 38 U.S.C. 303, and Chapter 5: Contracts and personal services, Title 38 U.S.C. 513.

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.

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
☒ Other Unique Identifying Number (list below)

☒ Administration (eg VHA, HSR&D, QUERI, etc.)
☒ General Job Role (e.g. Doctor, Administrative Staff, Nurse, etc.)
☒ Job Title
☒ Work Email Address
☒ Work Phone Number

PII Mapping of Components

DMVA does not have any components mapped. The DMVA leverages internal services-in-scope from AWS (Amazon Web Services)

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) 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

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.

Login is controlled via Active Directory Services for VA users. External users are guests and have an anonymous account that can only view public practice pages that have been allowed/approved by practice page owners.

Name, place of employment, general job role, job title, phone number, and profile picture are self-reported by each individual.

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.

Information about VA users are leveraged via Active Directory Services.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose.
This question is related to privacy control AP-2, Purpose Specification.

The content that is collected on the practice pages are used to populate the practice pages and provide proven best practices that can be of informational use or allow a user to implement a practice in their given location.

1.5 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.

All information is self-reported by users.

1.6 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

Users of DMVA sign the Terms and Conditions and agree to provide and allow DMVA to collect the required information to use the application. VA Privacy Service has determined the Privacy Act of 1974, 5 U.S.C. § 552a (e), Section 208©, E-Government Act of 2002 (P.L. 107-347), and the Office of Management and Budget (OMB) Circular A-130, Appendix I are the legal authority to permit the collection, use, maintenance and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.

DMVA is not a System of Record. Documents such as letters, memoranda, reports, handbooks, directives, manuals, briefings, or presentations are non-recordkeeping copies of documents stored in a System of Record. Users who post non-recordkeeping copies of records should make every effort to ensure such content is kept up to date and announce updates to copies of records. Users of non-recordkeeping copies of records should ensure that these copies are up to date, notify content owners when out of date or incorrect copies of records are found, and refer to the appropriate System of Record as needed. Transitory or intermediary records should be removed from DMVA and moved to a system of record as soon as these documents are complete. (see National Archives and Records Administration General Records Schedule sections 3.1, 3.2, 5.1, and 5.2).

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: There are some elements of PII that is collected from VA employees such as full name, VA phone number, VA email address. The bulk of the data is common practices that does not collect PII. PII required to use the system is managed by the OPM and publicly available, and PII not required to use the system is only submitted by users at their own discretion and can be removed or corrected at any time. If this information is breached or compromised, it poses a low risk of harm to the individual's professional, personal, and financial aspects of life.

Mitigation: Office of Security and Information (OSI) has an Information Security Officer and a Privacy Officer to assist and monitor in protecting the individuals' information.

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 information is collected allow the users to search for best practices within the DMVA.

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

Practice pages and practice partners can be sifted through using a search function that consists of keywords, and filtering to find the specific needs required. The search function is text-based and checkbox filtering to best match the practice page, no additional analysis of users or their data is performed.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

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

Practice Partners profiles are visible on the respective practice page along with name, work email address, job title, and profile picture (optional).

Site administrators will have access to all user information, including PII. Site administrators and moderators can screen commentary boxes and practice page updates to flag PII.

Section 3. Retention of Information

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

3.1 What information is retained?

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

Name, email address, general job role, place of employment, job title, and profile picture.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

User profiles, user content, and user group content are deleted when 5 years have passed since their last use. This content is governed by the National Archives and Records Administration (NARA) General Records Schedule (GRS) items 3.1. 3.2, 5.1, and 5.2. Items of these types are temporary and to be destroyed when their business use ceases.

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.

The owners of this system are working with the VA records office to create a retention schedule for review by NARA. The system currently removes user data after 5 years have passed since its last use.

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

SPI is eliminated after 5 years of user inactivity. This is done by deleting the user's profile including all SPI, any database entries and archives, and any documents owned by that user. These data are covered by NARA GRS items 3.1, 3.2, 5.1, and 5.2, which states that these data are temporary and should be destroyed after its business use.

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

PII is not used for research, testing, or training. Research, testing, and training occurs in our separate testing environment that does not contain PII.

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> The minimal PII that is collected from active VA employees is low risk and retention does not increase the risk.

<u>Mitigation:</u> Once an active VA employee no longer requires access to the site their account information to include PII is no longer retained after 5 years of inactivity.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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:

Mitigation:

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: This question is #7 in the Privacy Threshold Analysis.

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 data element types such as PII/PHI that are shared/received 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***

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

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

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

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:

<u>Privacy Risk:</u>

<u>Mitigation:</u>

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.

Notice is provided within the Terms and Conditions before signing up and collecting information. The Terms and Conditions must be accepted prior to inputting any information. A link of the DMVA Terms and Conditions is provided as Appendix A.

Here is a link to the Terms and Conditions:
https://github.com/department-of-veterans-affairs/diffusion-marketplace/blob/master/app/views/users/terms_and_conditions.html.erb

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 system cannot be used unless VA email address and password are provided with PIV authentication.

External users are anonymized with guest access and permissions.

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

Practice pages are read-only and can only be modified by practice page owners and appointed editors by the practice page owners. The content, pictures, and resource consumption that is made available for everyone to see can be modified by appointed editors with the appropriate permissions granted by the practice page owner.

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: Phone numbers and profile pictures are optional uses for user profiles and are Sensitive Personal Information. Users may not know that these are considered Sensitive Personal Information.

Mitigation: The DMVA Terms and Conditions informs users that work phone numbers and profiles pictures are considered Sensitive Personal Information, and risks associated with providing that type of information. Users are advised to not provide personal phone numbers or PII throughout the application.

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 would need to contact the Active Directory Services team to request any informational changes.

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 would need to contact the Active Directory Services team to request any informational changes.

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 would need to contact the Active Directory Services team to request any informational changes.

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.

This does not apply. Users are always able to correct their information.

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: The privacy risk related to access, redress, and correction is low. Use of the system is opt-in and information can be changed at any time by individual users.

Mitigation: As risk is low, a mitigation is not identified.

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.

Currently all individuals with a VA email address (VA staff and contractors) may access the system. Users have a PIV card that associates their account with Active Directory Services.

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 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.

There is no PII that is being stored in the application. Contractors will have access to sensitive data. These contractors are tasked with almost all the design and maintenance of the application. Sensitive data is stored in an encrypted database in Amazon PostgreSQL where contractor team has the understanding that the data in the database is owned by the VA, and the contractor team understands the contractual and legal responsibilities regarding the user data in the application.

Contractors do not sign a confidentiality agreement or a Non-Disclosure Agreement.

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.

All individuals working on the contract have completed the mandated VA Privacy training; Privacy and HIPAA Training and VA Privacy and Information Security Awareness and Rules of Behavior.

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

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*
4. *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.***

1. 11/24/2020
2. Conditional ATO
3. 1 year
4. Moderate
5. Status of 3 year:
    a. Nessus Scan to be completed monthly
    b. Penetration Test – Continue to remediate the findings, and scan annually.
    c. Database Scan – Continue to remediate the findings, and scan annually.
    d. Security Configuration Compliance Data (SCCD) – Ensure Bigfix is attached to all operating systems
    e. Security Documentation – Ensure all system security documentation is completed and uploaded to the Artifacts tab.

Section 9. 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.

Andrea J. Wilson 104706

Digitally signed by Andrea J. Wilson 104706
Date: 2021.06.21 12:38:15 -04'00'

Privacy Officer, Andrea Wilson

Merle L. Kelley 194113

Digitally signed by Merle L. Kelley 194113
Date: 2021.06.21 13:08:27 -05'00'

Information Systems Security Officer, Merle Kelley

Stefan G. Test 122392

Digitally signed by Stefan G. Test 122392
Date: 2021.06.21 14:55:52 -05'00'

System Owner, Stefan Test

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).

https://github.com/department-of-veterans-affairs/diffusion-marketplace/blob/master/app/views/users/terms_and_conditions.html.erb