Privacy Impact Assessment for the VA IT System called:

VBA Private Medical Records Portal

VBA Compensation Service
Veterans Benefits Administration

Date PIA submitted for review:

June 8, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jean-Claude Wicks	Jean-Claude.Wicks@va.gov	(202) 502-0084
Information System Security Officer (ISSO)	George L. Ragland III	George.Ragland@va.gov	973-297-3348
Information System Owner	Shaun Chelgreen	Shaun.Chelgreen1@va.gov	314-253-6876

Abstract

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

VBA Private Medical Records Portal is currently assigned the acronym DOMA. The vendor "DOMA Technologies, LLC (DOMA)" supports operations for the Private Medical Records (PMR) Retrieval Program. For that reason, the vendor will be referred in this document as "the vendor" rather than by name.

The program is deployed nationally and provides development assistance to VA Regional Offices (VARO) and Pension Maintenance Centers (PMC) in obtaining private medical records required to substantiate benefit claims for Veterans and their beneficiaries. The vendor's proprietary technology platform is Electronic Knowledge Database (EKDB), formerly known by VA as "iCharts." EKDB is commonly referred to by Veterans Benefits Administration (VBA) users as the "PMR Portal" and provides a centralized, single point of entry for all electronically date stamped requests to obtain private treatment records. EKDB resides outside of VA's network firewall. It does not interface with any VBA system or application. DOMA Technologies has established MOUs with Veterans Claims Intake (VCI) vendors, Systems Made Simple (SMS) and GENERAL DYNAMICS INFORMATION TECHNOLOGY (GDIT) to create bi-directional exchanges of information to automate transmission of requests at scan for immediate processing, and to ingest the treatment records (and other related documents) into the VBMS eFolder at completion of development.

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:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Please provide response here

VBA Private Medical Records Portal (DOMA); VBA Compensation Service

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

Please provide response here

DOMA is deployed nationally and provides development assistance to VA Regional Offices (VARO) and Pension Maintenance Centers (PMC) in obtaining private medical records required to substantiate benefit claims for Veterans and their beneficiaries.

C. Indicate the ownership or control of the IT system or project.

Veterans Benefits Administration, VBA Compensation Service

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

There are approximately 50,000 individuals with PII stored in the system. The typical client is a Veteran

E. A general description of the information in the IT system and the purpose for collecting this information.

Private medical records required to substantiate benefit claims for Veterans and their beneficiaries

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.

DOMA does not directly interface with any VBA system or application. The vendor has established MOUs with Veterans Claims Intake (VCI) vendors, SMS, and GDIT creating bi-directional information exchanges to automate transmission requests at scan for immediate processing and ingest the treatment records (and other related documents) into the VBMS eFolder at development completion

G. 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.

DOMA resides outside of VA's network firewall/network at the Vendor's QTS Datacenter

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

The legal authority to operate this system are SORN 58VA21/22/28; Title 10 U.S.C. chapters 106a, 510, 1606 and 1607; and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55

The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12.

I. 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 system is not in process of modification; it will be replaced by a cloud-based SaaS from the same vendor, with a separate ATO

J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*

Completion of this PIA will not result in processing changes

K. *Whether the completion of this PIA could potentially result in technology changes*

Completion of this PIA will not result in technology changes

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 Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☒ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☒ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

- Photographic Images

PII Mapping of Components (Servers/Database)

DOMA consists of 2 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by DOMA and the reasons for the collection of the PII are in the table below.

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.

Internal Database Connections

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
Server Name: dbpmr-east-1 **Database Name: PMR** **Batch File Import, and Document Repository**	**Yes**	**Yes**	**VAF 21-4142, Private Medical Records (Name, SSN, DOB, Previous Medical Records), & Other Medical Records Development Documents**	**(1) Obtain Veterans private medical records and (2) Return them for upload to the Veterans eFolder for evaluating disability claims. (3) Records are held 1 year after transmission to VBMS, then destroyed.**	**Secure File Transfer Protocol, System is operating with an ATO**

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Information is collected from sources internal to VA, such as Veteran's Private Health Providers (PHP) data uploaded to VBMS. Data can potentially be collected directly from the VAF 21-4142 request, a manual process. The VAF 21-4142 process is no longer used by VA but has not been removed from DOMA capabilities

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Data is required so the VA's Veteran benefits record has pertinent, updated medical information for providing the entitlement to benefits.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

DOMA does not create data

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Data in DOMA is collected from other VA sources via electronic transmission, not directly from Veterans. Transmission follows VA requirements (de-identification and/or encryption.

1.3b 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.

Information is not collected directly by DOMA

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

The information stored in the system is verified by DOMA using VBA's Share application. DOMA verifies the Veteran's profile information (SSN, DOB, etc.) on the VAF 21-4142 against VBA's Corporate database to ensure accuracy before processing the request. Once medical record development (letters, treatment records, reports of contact) is complete the data is transmitted to VCI, CM for subsequent upload into VBMS. DOMA returns a metadata file with the development documents for each Veteran record that is validated for accuracy against the corporate database.

1.4b 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.

DOMA does not access commercial information aggregators

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

The claimant's SSN is included on source materials provided by VA. As part of the Veterans Benefit Act, 38 U.S. Code § 7703 governed by the Code of Federal Regulations, 38 CFR §§ 1.575(b), 3.216 requires assisting claimants with adjudication, including obtaining private medical records on their behalf. Records are stored in VA's existing system of records ''Compensation, Pension, Education, and Rehabilitation Records"—VA (58VA21/22/28). Authority for system maintenance falls under Title 10 United States Code (U.S.C.) chapters 106a, 510, 1606 and 1607; and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55. VA's gathering and creating these records enables it to administer statutory benefits programs to veterans, service members, reservists, their spouses, surviving spouses, and dependents. Claims are filed claims for a wide variety of Federal benefits administered by VA.

Office of Management and Budget (OMB) Memorandum 07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", directs all Federal agencies to review and minimize use of SSNs. The President's Task Force on Identity Theft report "Combating Identity Theft: A Strategic Plan", released April 23, 2007, recommends reducing SSNs use by Federal agencies. The Administrations and Staff Offices developed

and implemented plans to reduce or eliminate the collection and use of SSNs except where a compelling business need is shown or the collection and use is authorized by law or deemed necessary to the mission of the Department, as described by the Secretary. VA Handbook 6507.1 "Acceptable Uses of the SSN", Paragraph 2, authorizes VA to collect the SSN to aid the retrieval of medical records from providers.

The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

Principle of Purpose Specification: 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: Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) contained on the system could potentially be accessed by unauthorized users.

Mitigation: The vendor maintains all paper or private medical records provided by the PHP. The requests, letters and private medical records are kept for at least 1 year after confirming the documents were successfully uploaded to VBMS. After 1 year, the following minimum guidelines are followed in destruction: paper records are pulped, macerated, or

shredded to a degree definitively ensuring they are not readable or reconstructable (no longer used). Final destruction must be performed by a National Association for Information Destruction (NAID) certified, bonded, and insured recycler or paper mill. Any intermediary processes must protect the records until final destruction is complete.

DOMA electronic records storage encrypts data on the system and retains the data for at least 1 year after confirming the documents were successfully uploaded to VBMS. The contractor is required to follow guidelines found in VA Handbook 6500 and 6371. All data and reports shall be transferred to VBA upon contract completion. Before termination or completion of this contract, Contractor will not destroy information received from VA, or gathered / created by the Contractor while performing this contract, without prior written approval by the VA / Contracting Officer. A Contractor destroying data VA data must do so in accordance with National Archives and Records Administration (NARA) requirements found in VA Directive 6300 "Records and Information Management", Handbook 6300.1, "Records Management Procedures", applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of contract termination. The guidance documents are available at: VA Publications Search List https://vaww.va.gov/vapubs/search_action.cfm?dType=1

Section 2. Uses of the Information

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

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

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

Name: identify and track individual(s) in VA systems Address: identify and track individual(s) in VA systems. SSN: identify and track individual(s) in VA systems. DoB: identify and track individual(s) in VA systems. Mailing Address: identify and track individual(s) in VA systems. Zip Code: identify and track individual(s) in VA systems. Previous Medical Records: identify and track individual(s) in VA systems; evidence for benefits claims. Death Certificate: identify and track individual(s) in VA systems

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

DOMA does not perform analysis of information within records. Medical records requests are provided to DOMA through electronic transmission from VCI, CM. Veteran profile information is provided to DOMA through a metadata file. Metadata can also be found on the medical records request. DOMA provides this form to PHPs for retrieval of medical records. After receiving the medical record package from the PHP DOMA verifies data against the original request for accuracy. All documents are returned to VCI, CM for storage in VBMS.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

DOMA does not create data

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

The PMR Portal and supporting servers reside on AWS GovCloud. As an AWS Advanced Partner, DOMA follows AWS Best Practices for safeguarding customer data. All data in transit is encrypted using Transport Layer Security (TLS) v1.2 and systems reside behind load balancers and web application firewalls (never directly accessible). All data at rest is encrypted with the Advanced Encryption Standard using 256-bit keys (AES-256).

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

Customer data entered into the PMR Portal Database is stored as encrypted strings using AES-128 encryption; this would include SSNs.

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

DOMA follows the rule of least privilege and access to the PMR Portal is restricted to business use only. The use of PII/PHI within the portal is outlined in contractual requirements and business units' access to specific metadata elements is restricted by role and task areas.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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.

2.4a How is access to the PII determined?

The information can only be accessed by DOMA employees who have background investigations completed at the correct level and have completed annual VA TMS security and privacy awareness training / rules of behavior. DOMA monitors and audit access by DOMA employees.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes (AC-2)

2.4c Does access require manager approval?

Access to the VA network and DOMA requires ISO / COR approval (AC-2.22), monitored by the vendor.

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

Access for DOMA personnel is monitored by monthly AD audits performed and recorded at access-hosting facilities; and by quarterly audits of Elevated Privileges performed and

recorded by access-hosting facility and VA Strong Authentication (oversees all Elevated Privileges). In addition, the vendor monitors, performs, and records access for personnel directly controlled by the vendor. Tracking and recording is made available to the ISO.

2.4e Who is responsible for assuring safeguards for the PII?

The vendor monitors and assures PII safeguards. Information transmitted to DOMA is the responsibility of the transmitter.

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*

DOMA retains: all private medical records and media (CD, USB, etc.) containing copies of PHP-provided medical records; and requests, letters and private medical records.

3.2 How long is information retained?

*In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods**. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Requests and records are kept for at least one year after confirming the documents were successfully uploaded to VBMS.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. 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. Please work with the system Privacy Officer and VA Records Officer to answer these questions.

This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

The vendor database which stores DOMA data is not a system of record; and the system of record for ingest of DOMA-related documents is VBMS.

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

The retention length is a contract requirement between VA and the vendor.

3.4 What are the procedures for the elimination or transfer of SPI?

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

DOMA electronic records storage encrypts data on the system and retains the data for at least 1 year after confirming the documents were successfully uploaded to VBMS. The contractor is required to follow guidelines found in VA Handbook 6500 and 6371. All data and reports shall be transferred to VBA upon contract completion. Before termination or completion of this contract, Contractor will not destroy information received from VA, or gathered / created by the Contractor while performing this contract, without prior written approval by the VA / Contracting Officer. A Contractor destroying data VA data must do so in accordance with National Archives and Records Administration (NARA) requirements found in VA Directive 6300 "Records and Information Management", Handbook 6300.1, "Records Management Procedures", applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of contract termination. The guidance documents are available at: https://vaww.va.gov/vapubs/search_action.cfm?dType=1 VA Publications Search List

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

N/A; DOMA information is never used for research, testing, or training

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

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

Follow the format below:

Privacy Risk: There is the potential that information contained in the system will be retained longer than is necessary to fulfill the VA mission.

Mitigation: All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually; data is stored at a secure data center which is monitored 24x7 and employs least privilege access controls.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: **Data sharing is necessary to obtain cycle time analytics for processing private medical record requests. There is a risk that data could be shared with an unintended VA organization.**

Mitigation: **Information is shared per VA Handbook 6500. User accounts require PIV MFA; all user actions within the application are audited.**

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	***List the purpose of***	***List the specific PII/PHI data elements that are processed***	***List the legal***	***List the method of***

or IT System information is shared/received with	*information being shared / received / transmitted with the specified program office or IT system*	*(shared/received/transmitted) with the Program or IT system*	*authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*transmission and the measures in place to secure data*
Government CIO (GCIO)	**1) Process VAF 21-4142 for private medical records development 2) Return the records to VBA for disability claims evaluation**	**Veteran's Name, Personal Mailing Address, Social Security Number, Personal Phone Number, Certificate / License number, Date of Birth, Date of Death, e-mail, claim ID, and other information required to complete VA Form 21-4121.**	**ISA/MOU exist between DOMA vendor and GCIO.**	**Secure File Transfer Protocol (SFTP)**

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: Privacy information may be released to unauthorized individuals.

Mitigation: **Contracted personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. Information is shared per VA Handbook 6500.**

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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (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?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a 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, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

DOMA Does not directly collect veteran PII. Veterans request the release of their information, so are aware their data has been collected. By official process, data is originally collected on VA information release forms, "Authorization and Consent to Release Information to the Department of Veterans Affairs" Veterans requests their Primary Health Provider release the information to the Department of Veterans Affairs. The form describes information use and that the authorization may be revoked at any time.

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
DOMA Does not directly collect veteran PII; and cannot provide copy of current notices in place for other PII collectors. By official process, data is originally collected on VA information release forms, "Authorization and Consent to Release Information to the Department of Veterans Affairs" Veterans requests their Primary Health Provider release the information to the Department of Veterans Affairs. The form describes information use and that the authorization may be revoked at any time.

Please provide response here
6.1c 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.

DOMA Does not directly collect veteran PII; and cannot describe PII collection processes used by individual collectors. By official process, data is originally collected on VA information release forms, "Authorization and Consent to Release Information to the Department of Veterans Affairs" Veterans requests their Primary Health Provider release the information to the Department of Veterans Affairs. The form describes information use and that the authorization may be revoked at any time.

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.

Veteran must authorize VA to collect private medical records information from their Primary Health Provider (PHP). Without authorization medical records are not obtained by VA. PHP may decline to provide records for a number of reasons, to include: cost (VA does not pay for medical records); PHP requires an additional release form; or, the records have already been provided.

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 Veteran consents information use when completing VA form, "Authorization and Consent to Release Information to the Department of Veterans Affairs".

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

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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 an individual may not be notified their information is being collected, maintained, processed, or disseminated.

Mitigation: The VA has no knowledge of the information until it is provided by the PHP; The PHP only sends the information after VA form 21-4142 is completed and signed by the Veteran. The 3 main forms of notice are discussed in detail in question 6.1 and include the Privacy Act statement and the publishing of this Privacy Impact Assessment.

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?
These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at https://www.va.gov/foia/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

DOMA is not in direct contact with veterans and does not collect veteran data. No procedures / regulations can be created internally which would allow them access to information stored by DOMA; all information in DOMA is accessible through data collectors. At an enterprise level, veterans may visit the nearest VA Regional Office, or go to www.va.gov/benefits to obtain copies of their records

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

DOMA is not exempt from the Privacy Act

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

N/A

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.

DOMA is not informed of inaccurate or erroneous information; it must be corrected by data collectors. Veterans can call a VA representative at (800) 827-1000 xtn 0, visit the nearest VA Regional Office, or go to www.va.gov/benefits to correct inaccurate or erroneous information.

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.

During data collection Veterans are advised of intended information use. The VA website www.va.gov/benefits provides instructions for correcting information, as well as speaking to a VA representative at the nearest Regional Office or at (800) 827-1000 xtn 0.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

DOMA is not in direct contact with Veterans and cannot provide redress processes. The Veteran can speak with a representative at (800) 827-1000 xtn 0, or obtain alternative

information such as specific contact information for specific benefits, such as Education, Vocational Rehabilitation & Employment, etc. from the VA website, www.va.gov/benefits

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

Privacy Risk: There is a risk that Veterans/ members of the public will not know the procedures for gaining access to, correcting, or contesting their information.

Mitigation: The Veteran can speak with a representative at (800) 827-1000 xtn 0 or obtain alternative information including contact information for specific benefits such as Education, Vocational Rehabilitation & Employment, etc. from the VA website www.va.gov/benefits .

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?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

Physical and logical access to DOMA is limited to personnel with completed security requirements including a background investigation, drug screening, and US citizenship. Physical access controls include keycard locked doors and closed-circuit television monitoring. Logical access is enforced using MFA. Once authenticated, authorization levels are role-based using best practices (e.g., least privilege, separation of duties). For example, people who access the operating system do not have access to the database, and vice versa. DOMA security processes and procedures are documented in the DOMA Information Security Program Plan. Control details are documented in DOMA System Security Plan.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Users from outside of the VA do not have access the system

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Information in DOMA is not modified while in the system. Vendor System Admins have EP access to the system for patching, etc.; VA and vendor supervisors currently have read-only access. No VA sysadmins work on DOMA

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.

DOMA designed, developed, and operates DOMA DX as a Commercial Off The Shelf (COTS), Software as a Service (SaaS) Product. DOMA DX v8 is the platform for the PMR Portal.

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.

DOMA, a contractor to VA, owns and operates the EKDB system. Physical and logical accesses to the system are restricted as documented in Section 8.1. Physical and logical access is restricted to DOMA employees and vetted contractors only. A vetted contractor is someone who has meet all security requirements including a background investigation, drug screening, and US citizenship. Visitors, such as auditors, must coordinate with the security office before accessing the facility. When accessing the facility, they must show proof of US citizenship and be escorted by a DOMA employee at all times. VA contracts are reviewed yearly by Contracting Officer Representatives (CORs).

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

8.4a If Yes, provide:

1. *The Security Plan Status:* **SSP is current and approved**
2. *The System Security Plan Status Date:* **17 Nov 2022**
3. *The Authorization Status:* **ATO**
4. *The Authorization Date:* **17 Nov 2022**
5. *The Authorization Termination Date:* **15 May 2023**
6. *The Risk Review Completion Date:* **17 Nov 2022**
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* **Moderate**

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service

(MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

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). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

N/A

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

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

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

N/A

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

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

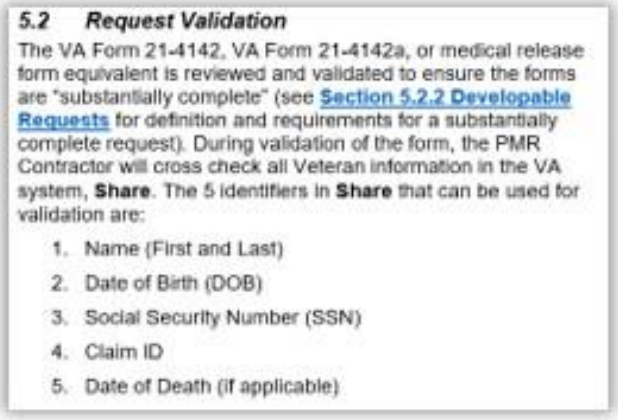
N/A

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

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

The proposed RPA/BOT will not run directly on VA systems, as such, the RPA will be running locally from within DOMA using a PIV card with VBMS access (Ref: Workflow below):

1. **DOMA RPA logs in through the Citrix Access Gateway (CAG) via PIV.**
2. **DOMA RPA logs into VBMS using the established BOT account.**
3. **DOMA's requirement is to validate/verify Veteran information in VBMS in-lieu of Share, validating the information provided on the Veterans 21-4142 form (Ref: Request Validation)**



5.2 Request Validation

The VA Form 21-4142, VA Form 21-4142a, or medical release form equivalent is reviewed and validated to ensure the forms are "substantially complete" (see **Section 5.2.2 Developable Requests** for definition and requirements for a substantially complete request). During validation of the form, the PMR Contractor will cross check all Veteran information in the VA system, **Share**. The 5 identifiers in **Share** that can be used for validation are:

1. Name (First and Last)
2. Date of Birth (DOB)
3. Social Security Number (SSN)
4. Claim ID
5. Date of Death (if applicable)

4. **DOMA's RPA would then launch its DX software into a tab, copying and pasting the specific validation fields between VBMS and DX within the browser (e.g., in the remote desktop).**

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

JEAN-CLAUDE WICKS

Digitally signed by JEAN-CLAUDE WICKS
Date: 2023.07.17 05:37:35 -06'00'

Privacy Officer, Jean-Claude Wicks

GEORGE L RAGLAND 3455835

Digitally signed by GEORGE L RAGLAND 3455835
Date: 2023.07.17 08:26:56 -04'00'

Information Systems Security Officer, George L. Ragland III

SHAUN CHELGREEN

Digitally signed by SHAUN CHELGREEN
Date: 2023.07.17 08:49:01 -04'00'

Information System Owner, Shaun Chelgreen

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).

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices