Privacy Impact Assessment for the VA IT System called:

Member Services Publication Store

VHA Member Services

Date PIA submitted for review:

1/301/2020

System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Janet Asafo	Janet.Asafo@va.gov	404-828-5307
Information System Security Officer (ISSO)	Howard Knight	Howard.Knight@va.gov	404-828-5340
Information System Owner	Darryl Jones	Darryl.Jones2@va.gov	404-828-5810

Abstract

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

The store is a place where VA employees can select publications that they need for Veterans' information, order the specific quantities that they need at their facility. The store is used as a compiling location to generate a mailing list so that we have a list of current addresses and limit the distribution on only copies that are needed. This greatly reduces waste and returned shipments. The purpose of the Member Services (MS) Publication Store is for internal VA customers to submit print orders for specific VA documents and publications. It is meant to reduce the expense of overrun printing and ensure the most up to date publications are available.

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 Veterans Health Administration (VHA) Member Services (MS) Publication Store is a VA wide system owned and operated by VHA Member Services. The purpose of the Publication Store is to allow VA employees a centralized location where they may request printed copies of VHA MS publications. The Publication Store is a stand-alone application where VA employees create a registration account (name, work address, work phone) that is recorded within the system. VA employees request a publication and the registered information is used to fulfill the delivery of the request.

This store operates so that facilities may obtain copies of publications to fulfill the mission of VA and has no other legal authorities. The system does not interface with any other systems (VistA, VA database, etc.)

If the information were disclosed, only current VA employee work address and phone numbers would be exposed. The number of individuals whose information is stored in the system varies based on the number of subscriptions submitted by VA employees.

The completion of this PIA will not result in circumstances that require changes to business processes nor will it 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 (Enter website _____). 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)

Director, Health Eligibility Center
VHA Member Services
2957 Clairmont Road
Atlanta GA 30329
Tel: 404-828-5302

PII Mapping of Components

The MS Publication Store consists of 2 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the MS Publication Store and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Components of the information system (servers) collecting PII	Does this function collect or store PII? (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
Publication Store Web Site	**Yes**	**Name, mailing address, VA Network User ID, VA phone number, VA email address**	**Delivery point of requested documents**	Information System complies with NIST 800-53 requirements including database encryption and application secure code review.
Publication Store Database	**Yes**	**Name, mailing address, VA Network User ID, VA**	**Delivery point of requested documents**	Information System complies with NIST 800-53

		phone number, VA email address		requirements including database encryption and application secure code review.

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.

Information is self-provided by employee requesting printed document.

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 collected upon registration is as follows: First name, Last Name, VA Network User ID, Employee VA Email Address, Employee VA Phone number, Facility Address (for shipping). Other stored information will be number of copies of a requested publication when the VA employee makes a request.

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 purpose of the information collected is to facilitate the distribution of VHA MS publications to field facilities. By maintain the database of actual requested number of publications VA has reduced waste through the reduction of excess or wasted copies and return shipments from unwanted or incorrect deliveries.

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.

Since this system is a user requested ordering system, the user is requested to verify their information each time they place an order. There are no other checks.

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

The authority is the Government Printing and Binding Regulations of the Joint Committee on Printing, under authority of section 103, 501, and 502, title 44, USC.

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:

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: The risk of exposing the information would expose VA employee work phone and facility addresses.

Mitigation: The system is behind VA firewall and is not accessible from outside the VA network. Internal security measures include access control, awareness and security training, identification authentication, physical and environmental protection.>>

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: The name is used to identify the employee (requester) requesting the publication.

Mailing Address: The mailing address is used to send the publications to the requester.

Zip Code: The zip code is a part of the mailing address and is used to send the publications to the requester.

Phone Number: The phone number is the number belonging to the requester and is used to contact them if additional information is needed or there are questions or special instructions about their request.

Email Address: The email address is the requester's email address and remains internal only and are utilized when communication needs to occur between the store and the customer or, more commonly, is

used as the return email address when the customer submits a question to the publication owner or IT support through the store interface.

Network User ID: The network ID is the requesters ID and remains internal to the VA.

The business purpose of the Member Services On-Line Store is to gather custom shipping lists for VA/MS publications only. The information gathered is limited to requestor's name, shipping address and contact information. This information is then compiled into a shipping list and provided to a printer through the GPO for printing and distribution. Information is necessary for delivery of the requested products.
Contact information (phone number) is provided to the delivery company and the email address stays inhouse for communication through the store in VA only. Clauses are placed in the contract that the information may not be used for other purposes and is to be destroyed within 30 days of completion of the project.

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

This is a self-contained, user driven system. There are no tools to analyze data.

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

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

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

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

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

Add answer here: Only administrators have full access to the database which houses VA Employee information. Administrators are required to complete initial and annual mandatory online information security and Privacy and HIPAA Focused training and sign the VA Information Security Rules of Behavior.

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

Information collected upon registration is as follows: First name, Last Name, VA Network User ID, Employee VA Email Address, Employee VA Phone number, Facility Address (for shipping).

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.

Information is retained under Records Control Schedule (RCS) 2525.2. Hence records will be destroyed when 1 years old, or when superseded or obsolete, whichever is applicable, but longer retention is authorized if required for business use (DAA-GRS-2016-0012-0002).

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.

Yes, the retention schedule has been approved by NARA and recorded under DAA-GRS-2016-0012-0002.

3.4 What are the procedures for the elimination of SPI?

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

Records can be destroyed after 1 year but based on business needs records are not destroyed and remain in system.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy of 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

Information is not repurposed for any other reasons.

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

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

<u>Principle of Data Quality and Integrity:</u> Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:
Privacy Risk: Consistent with business needs, there is no period for removal of records.

Mitigation: Only information required is stored in the system behind VA Firewall. Access is restricted to only VA employees with an operational requirement need to know. All information is maintained and protected in accordance with VA and Federal privacy regulations.

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.

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***
None	None	None	None

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:
Privacy Risk: No information shared internally.

Mitigation: <<ADD ANSWER HERE>>

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 #6 and #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

List External Program Office or	***List the purpose of information being***	***List the specific data element types***	***List the legal authority, binding***	***List the method of transmission and***

IT System information is shared/received with	***shared / received / transmitted with the specified program office or IT system***	***such as PII/PHI that are shared/received with the Program or IT system***	***agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***the measures in place to secure data***
Government Publishing Office (GPO) Print Vendor	Fulfill shipping or requested publications	Employees name, email address, work phone number, work facility name and main address appropriate to the agreement	Fulfillment of VA mission to educate Veterans	Secure File Transfer Protocol (SFTP)

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

N/A - Collected information is not accessed remotely or stored offsite and does not require additional specific measures IAW reference OMB Memoranda.

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: Exposure of VA Employee Name, work address and Work Phone number>>

Mitigation: Specific security language is placed in contracts to limit vendor use and destruction processes.

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.

VA provides notice to Veterans and their dependents on what information is collected on them and what that information is used for. This notice is provided in the Notice of Privacy Practices VA 10-163. Link provided in the appendix.

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

All information is voluntary to receive VA publications as requested by VA employees.

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

By placing an order, a user is requesting that the delivery information be used to fulfill the request.

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

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

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

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: A notice is not provided to the Veteran or public because this is a system internal to VA employees only.

Mitigation: VA mitigates this risk by ensuring user rights to access the reporting is limited by system permissions.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

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

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

The VA employee may see their registration information and previous orders any time they log into the system.

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.

If user made an error, they may correct it themselves since the store is self-service. When the individual registers their profile, they select their facility from the drop-down list of available facilities as populated from the VA Directory that was imported. The employee does not change that address unless they change their profile. The shipping address is displayed during the order confirmation to confirm the correct address. If the address is listed incorrectly, the employee may return to their profile and alter their facility.

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.

Employees are responsible to ensure their contact/delivery information is valid. It is a self-service interface. Employees may only select addresses from a drop-down list of VA facility addresses. If the address they are requesting is not in the list, they may email the webmaster to have it added once verified as a VA address. If the employee selects an incorrect address, materials will deliver as requested. The employee may change their address by entering their profile and selecting the proper address.

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.

If user made an error, they may correct it themselves since the store is self-service. When the individual registers their profile, they select their facility from the drop-down list of available facilities as populated from the VA Directory that was imported. The employee does not change that address unless they change their profile. The shipping address is displayed during the order confirmation to confirm the correct

address. If the address is listed incorrectly, the employee may return to their profile and alter their facility.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that information may be used for purposes other than for what it was provided
or agreed to.

Mitigation: Access to the information is limited based on user rights levels. Only elevated users have access
to reporting features or other user information.

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.

Only VA employees on the VA network may access the system.

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.

Any VA employee and contractors on the VA network may access the store. Only individuals with Administrative rights may access the database beyond the single user information.

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.

VA employees with access to VA sensitive information are required to take the VA Privacy and Information Security Awareness and Rules of Behavior training annually, as well as Privacy and HIPAA Focused Training.

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.***

An Authorization and Accreditation is not required for this system because it is not classified as a major application. A 180-day ATO was granted for the Health Eligibility Center (HEC) - Region 6 on September 1, 2020.

Section 9. References

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.

Asafo, Janet K. Digitally signed by Asafo, Janet K. Date: 2020.11.10 08:30:13 -05'00'

Privacy Officer, Janet Asafo

Knight, Howard (HEC ISO) Digitally signed by Knight, Howard (HEC ISO) Date: 2020.11.09 08:06:43 -05'00'

Information System Security Officer, Howard Knight

Darryl T. Jones 248911 Digitally signed by Darryl T. Jones 248911 Date: 2020.11.06 12:48:27 -05'00'

Information System Owner, Darryl Jones

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).

Notice of Privacy Practices VA Poster 10-163

Welcome to the Member Services' (MS) on-line ordering page. Use of the on-line ordering page enables VA to reduce the expense of overrun printing and assures the most up-to-date publication when you order.

MS will be printing and distributing certain documents periodically (monthly, quarterly, semi-annually) and for Initial Distributions (ID). Between MS requested print orders, you will be able to place your order on this site. Your order will be grouped with others and sent to the printer once the ordering period has closed. Please allow 4 - 6 weeks for delivery from the close date. See each item for ordering periods. You will be asked to select the publication and order your quantity.

Each Publication will have a specific point of contact that you may reach out to for assistance with the particular publication. If you have a question, click on the "text bubble" at the bottom of the publications' page. This will open a dialog box. Once you click "send" an email will be sent to that publication owner. The owner will respond directly to your email that is in your profile.

Each of our books are available for download as a PDF or to an eReader or eReader application free of charge. These books are available on our ePublications page (http://www.va.gov/healthbenefits/resources/epublications.asp) or Apple iTunes Book store.

Some materials on this site are available from the Service and Distribution Center via FPOrders. These publications must be ordered through the FPOrders system. Any item that lists FPOrders as the ordering chain will not be fulfilled through this portal. For ordering information please see http://vaww.va.gov/oal/sdc/formsPublications.asp

Other items are listed as "Local Reproduction Authorized". These items will not be fulfilled through this site. The link to the reproduction files will be in the description of the product which facilities may download and print locally.

All information provided (Name, address and contact information) is gathered to create a distribution list and will be provided to a third-party printer for the express purpose of distributing the publications as you have requested. Your information will not be used for any other purpose than fulfilling your requested orders.