Privacy Impact Assessment for the VA IT System called:

Intelliworx Application Management System - Enterprise

Veteran’s Health Administration

Workforce Management and Consulting Office

eMASS ID: 1103

Date PIA submitted for review:

02/23/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Harash Katyal	Harash.katyal@va.gov	(908) 864-3107
Information System Security Officer (ISSO)	Steve Cosby	Steve.Cosby@va.gov	(919) 474-3928
Information System Owner	Chino L. Walters	Chino.Walters@va.gov	(202) 461-0452

Abstract

The abstract provides the simplest explanation for "what does the system do?".

Intelliworx Application Management System – Enterprise (Intelliworx-E) is a SaaS solution that leverages technology to improve transparency, accountability, and agency reporting capabilities while streamlining operations for the Health Professionals Scholarship Program (HPSP), Employee Incentive Scholarship Program (EISP), Scholarship & Clinical Education (S&CE) program waivers, VA Student Trainee Experience Program (VASTEP) program, Special Education Loan Repayment Program (SELRP), and Visual Impairment and Orientation and Mobility Professional Scholarship program (VIOMPSP). Additional benefits of automation include timeliness throughout the entire application cycle, ease of use for the customer, centralized library content for standardization and consistency, and transparent record keeping with complete audit ability. The system will be used by approximately 8,000 scholarship applicants and 300 waiver applicants annually.

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. *What is the IT system name and the name of the program office that owns the IT system?*
Intelliworx Application Management System – Enterprise and Veteran's Health Administration (VHA) Workforce Management and Consulting Office

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

Provide Health Professional Education Assistance

C. *Who is the owner or control of the IT system or project?*

The VHA Human Capital Management (HCM) Office owns Intelliworx Application Management System – Enterprise (Intelliworx-E)

2. *Information Collection and Sharing*

D. *What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?*
Approximately 8,000

E. *What is a general description of the information in the IT system and the purpose for collecting this information?*

Intelliworx is an Application Management System (AMS) for the Department of Veterans Affairs (VA) that leverages technology to improve transparency, accountability, and agency reporting capabilities while streamlining operations for the Health Professionals Scholarship Program (HPSP), Employee Incentive Scholarship Program (EISP) and Scholarship & Clinical Education (S&CE) program waivers. Additional benefits of automation include timeliness throughout the entire application cycle, ease of use for the customer, centralized library content for standardization and consistency, and transparent record keeping with complete audit ability.

F. *What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.*
Intelliworx-e shares information with VA Identity and Access Management Assessing for user authentication. No external sharing is conducted with other entities.

G. *Is 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?*
Yes, the system is operated in more than one site. Global address book is shared across all sites and same security controls are used across all sites.

3. Legal Authority and SORN

H. *What is the citation of the legal authority to operate the IT system?* AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501(a).
Legal Authority: Privacy Act of 1974, 5 U.S.C 552a, as amended;
Intelliworx is covered under the SORN 161VA10 / 88 FR 42005 (Veterans Health Administration Human Capital Management-VA)
https://www.oprm.va.gov/privacy/systems_of_records.aspx.

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?*
No

4. System Changes

J. *Will the completion of this PIA will result in circumstances that require changes to business processes?*
No

K. *Will the completion of this PIA could potentially result in technology changes?*
No

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.

5.1 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. It must also match the information provided in question 3.4 of the PTA.

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[1]
☐ 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)

Other PII/PHI data elements:

PII Mapping of Components (Servers/Database)

Intelliworx-E consists of one key components (servers /databases /instances /application s/software /application programming interfaces (API). Each component has been analyzed to determine if any

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

elements of that component collect PII. The type of PII collected by Intelliworx-E 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 server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**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**
Intelliworx Cloud Workflow Platform (HR Worx)	Yes	Yes	• Name • Social Security Number • Date of Birth • Mailing Address • Mother's Maiden Name • Phone Number(s) • Email Address • Emergency Contact Information • Financial Account Information • Certificate/ License Numbers • Race/ Ethnicity • Gender • Next of Kin	File Identification and Scholarship Processing	https over port 443, validated user(s)

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?
System only collects information directly from VA employees, contractors and clinical trainees. No commercial data aggregators are used.

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.
System only collects information directly from VA employees, contractors and clinical trainees.
No commercial data aggregators are used.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
The system will create new standalone records about applicants of the health professional scholarship program (HPSP) and ESIP programs and their associated waiver requests. The information will be used to determine the applicant's suitability for the HPSP and Employee Incentive Scholarship Program (EISP) program, determine if they will be accepted into the program, ensure they are meeting the program requirements, and process waiver requests to approve contract breaches.

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?
Information is directly collected from the individual. Prior to submission, the applicant certifies that all information provided is true and correct to the best of their knowledge.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

As part of the Paperwork Reduction Act, the applicants will enter the information requested in VA Forms 10-0491, 10-0491A, 10-0491C, 10-0491D, 10-0491E, 10-0491F, 10-0491G, 10-0491H, 10 0491I, 10-0491J, 10-0491K and 10-0491L directly into the Intelliworx system.

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.
Prior to submission, the applicant certifies that all information provided is true and correct to the best of their knowledge.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?
Prior to submission, the applicant certifies that all information provided is true and correct to the best of their knowledge.

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

Title 38, United States Code, Section 17.600–17.612, 17.625-17.636, 17.640-17.6.

1.6 <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. (*Work with your System ISSO to complete this section)*

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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.

<u>Privacy Risk:</u> Due to the sensitive nature of this data, there is a risk that, if the data were accessed or received by unauthorized parties/recipients or otherwise breached, serious personal, professional and/or financial harm may result for the affected individuals. The Contractor or VA would be required to provide credit monitoring and ID theft insurance.

<u>Mitigation:</u> The system is FedRAMP certified to ensure the proper controls are in place for a FISMA moderate level to include encryption to secure data at rest and transit; user information security and privacy education and training; weekly administrative rounds to identify any potential issues, security screens and secure mailing. These measures also include, access controls, security assessments, contingency planning, incident response, system and communications protection. The system employee all security controls in the respective high impact control baseline unless specific exceptions have been allowed based on the guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA direct.

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 that 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.

PII/PHI Data Element	Internal Use	External Use
Name Social Security Number Date of Birth Mailing Address Mother's Maiden Name Phone Number(s) Email Address Emergency Contact Information Financial Account Information Certificate/License Numbers Race/Ethnicity Gender Next of Kin	File Identification Scholarship processing purposes	Not used

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?

The system will create new standalone records about applicants of the HPSP and ESIP programs and their associated waiver requests. The information will be used to determine the applicant's suitability for the HPSP and EISP program, determine if they will be accepted into the program, ensure they are meeting the program requirements, and process waiver requests to approve contract breaches.

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?
The new information will be used to determine the applicant's suitability for the HPSP and EISP program, determine if they will be accepted into the program, ensure they are meeting the program requirements, and process waiver requests to approve contract breaches. New information will be a part of the individual's existing record.

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?
Intelliworx application session traffic is encrypted utilizing Transport Layer Security (TLS) 1.2 and a FIPS 140-2 validated OpenSSL module.
Intelliworx system data is securely stored in the Intelliworx system MySQL database and encrypted through use of AWS GovCloud Infrastructure as a Service (IaaS) database encryption services.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
Full SSNs are hidden when users of the system view applicant information. Data at rest and transmit is also encrypted to protect the unauthorized access of PII.

2.3c How is PII/PHI safeguarded in accordance with M-06-15?
Single Sign-On (SSO) – Administrators can configure Cisco Webex Services to work with their existing SSO solutions. Cisco Webex Services supports identity providers using Security Assertion Markup Language (SAML) 2.0 and Open Authorization (Oauth) 2.0. Directory synchronization – Administrators can have employee lifecycle changes reflected in Cisco Webex Services in real-time when using Microsoft Active Directory
The Intelliworx system protects the confidentiality and integrity of data residing in system databases using encryption. The Intelliworx system operates on the Hrworx platform within, and leverages, the AWS GovCloud Infrastructure as a Service (IaaS) environment. Intelliworx leverages AWS Relational Database Service (RDS) functionality providing encryption that is inherited by the Intelliworx system. The AWS GovCloud IaaS maintains a FedRAMP Authorized package (ID F1603047866) providing statements describing AWS GovCloud IaaS implemented encryption controls. Please refer to the AWS GovCloud FedRAMP Authorized package for details.

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?

Compartmentalized access control to ensure data is only authorized to be viewed based on one of these criteria: facility managers, security specialist, waiver specialist, selection committee members, HR specialist, program specialist and superusers.

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

Documented on internal trackers for selection committee members and facility managers. Updated authorized users are requested via email and trackers are updated to reflect the changes. Other roles and authorizations are determined primarily by position assignment and the need to access required by position descriptions.

2.4c Does access require manager approval?

Yes

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

Access to PII is constantly being monitored and adjusted as request are constantly being made by users. The primary Super User functionality is being reviewed quarterly by program leadership.

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

Cloud Service Provider

Section 3. Retention of Information

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

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*

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

- Name
- Social Security Number
- Date of Birth
- Mailing Address
- Mother's Maiden Name
- Phone Number(s)
- Email Address
- Emergency Contact Information
- Financial Account Information
- Certificate/License Numbers
- Race/Ethnicity
- Gender
- Next to Kin

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.*

Program policy requires the information to be retained for 3 years after completion of the applicant's service obligation period. So, the maximum length would be 16 years for a first-year medical student. Average retention time would be around 8-10 years.

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?

Yes. The retention schedule has been approved by the NARA. The guidance for retention of records is found in the Records Control Schedule 10-1 http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf and NARA: https://www.archives.gov/records-mgmt/grs.html

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

According to VA Handbook 6500, once records are entered into the system they remain as part of the protected system information. System logs are maintained for one year and then flagged for deletion by their automated processes. System logs are not retained after one year and any SPI containing them will be overwritten as part of the process for audit management. When virtual machines are no longer required to support the system, they are wiped clean, and the data overwritten. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf In addition, any equipment that is decommissioned and is leaving the controlled data center will be sanitized (e.g., degaussing) or destroyed in accordance with VA Handbook 6500 and the Veterans Affairs Dedicated Cloud Media Sanitization Procedure. VA Dedicated Cloud Media Sanitization policy outlines the VA Dedicated Cloud policy and procedure for tracking, documentation, and disposal of storage media within the environment and their return to the VA, in accordance with VA Handbook 6500.

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.

The records will be permanently deleted from the system using a NIST 800-88 Standard for Data Wiping. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

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

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

Full SSNs are hidden when users of the system view applicant information. Data at rest and transmit is also encrypted to protect the unauthorized access of PII.

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 a risk that the information maintained in Intelliworx will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed in Intelliworx is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary.

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***
Identity and Access Management Assessing	For user authentication	Email address	HTTPS

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:

<u>Privacy Risk:</u> There is a risk that the data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy.

<u>Mitigation:</u> The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, program management, planning and maintenance. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external***	***List the method of transmission and the measures in place to secure data***

	office or IT system		***sharing (can be more than one)***	
Intelliworx Cloud Workflow Platform (HR Worx)	Information system reside outside VA.	• Name • Social Security Number • Date of Birth • Mailing Address • Mother's Maiden Name • Phone Number(s) • Email Address • Emergency Contact Information • Financial Account Information • Certificate/ License Numbers • Race/ Ethnicity • Gender • Next of Kin	SLA and ISA/MOU	Electronic File Transfer

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

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

Follow the format below:

<u>Privacy Risk:</u> There is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

<u>Mitigation:</u> The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, program management, planning and maintenance. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

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.

Upon access of the system, users will be notified this is a U.S. Government computer system that contains sensitive information and is for official use only. Activity on this system is monitored. Use of this system constitutes your unconditional consent to such monitoring and no expectation of privacy. Misuse of, unauthorized access to, or attempted unauthorized access to this system will result in administrative disciplinary action and/or criminal prosecution as appropriate. System of records notice *Veterans Health Administration Human Capital Management (161VA10 / 88 FR 42005)*

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Notice is provided.

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.

Throughout the system, there are numerous Privacy Act, Data Collection Requests, FAFSA Release, and Authorization to Release Information forms that are required to be signed and maintained with the system to provide the leeway to gather, review, and collect additional information as required.

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.

Potential applicants can decline to provide information if they don't want to apply for the scholarship programs we offer. Applicants that have been accepted into the program are legally bound to provide information to meet program requirements to prevent a breach in contract.

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 information is required to apply for the scholarship programs. The system does not provide the applicant the ability to choose how their applicant information is used. However, an applicant, guardian or court appointed Power of Attorney can submit a request to a VHA Privacy Officer to restrict usage.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (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 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: There is a risk that an individual providing the information may not read the Notice when signing into their account.

Mitigation: The user is required to agree to the terms before they can move forward with entering their information.

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 http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

The individual will retain access to the information they entered into the system until the record is destructed at the end of its retention period. A FOIA request can be submitted by the individual using the instructions listed on http://www.foia.gov/how-to.html.

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)?
This system is not exempt from provisions of 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?
This is a Privacy Act 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.

Prior to submission of the application and the applicant's certification that they attest the information provided is true to the best of their knowledge, the applicant can update the information themselves. After the application has been submitted, the applicant can only view the information and can submit a Help Desk request for the information to be updated.

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.*

> After an individual submits their application, they will be able to view the application in a read-only mode and will be presented with instructions on how to contact the help desk for assistance in correcting information in a previously submitted application. There will be no need to change information after an application is approved or denied as it will not affect the status of the application.

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.

> The individual will retain access to the information they entered into the system until the record is destructed in accordance with program retention periods. Prior to submission of the application and certification that they attest the information provided is true to the best of their knowledge, the applicant can update the information themselves. After the application has been submitted, the applicant can only view the information and can submit a Help Desk request for the information to be updated.

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.

Privacy Risk: Individuals will be unable to receive assistance from Help Desk to correct their application.

Mitigation: The Help Desk will be available Monday – Friday from 8am-5pm ET to assist with access, redress and correction requests.

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?

By default, applicants can only see the information they entered into the system. For other role assignments, the Help Desk has a document process for the approval of roles that is based on an individual's job duties with respect to the application. Quarterly system permission reviews will also take place as a part of VA ATO and FedRAMP security requirements.

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?

No users from other agencies have access to this 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.

- Global Administrator(s): Overall site development and template management.
- Manager User(s): Ability to manage system access based on restrictive levels of original access (i.e., facility assignment).
- Facility Coordinator User(s): Each facility in the VA will have access to manage VASTEP application/waiver lifecycle and be limited to facility specific tasks.
- Program Specialist Account(s): Specific accounts to program manage different aspects of the application/waiver lifecycle. These accounts include but are not limited to Financial, Program Support, Waiver, Application Reviewer, Program Manager/Director, Selection Committee Chairmen etc.
- Selection Committee User(s): Users that will review, rate and rank applicants.
- External Data Provider(s): The ability to have 3rd Party inputters of application data as requested by the applicant. This includes but is not limited to Academic Verification, References, Change approvers, etc.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

> Yes, this a vendor-hosted, cloud based, SaaS solution that VA contractors will have access to. The contractors will be responsible for system maintenance, upgrades and help desk support. The contractors will sign an NDA when the contract is awarded.

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.

> Yearly training is required for all users including additional training for managing PII and paperwork for PII including VA Privacy and information security awareness and rules of behavior and Annual Government Ethics Training.

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

8.4a If Yes, provide:

1. *The Security Plan Status: Approved*
2. *The System Security Plan Status Date:* 11/16/2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 04/10/2023
5. *The Authorization Termination Date:* 04/09/2925
6. *The Risk Review Completion Date:* 03/22/2023
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.***

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)*

Yes, this is a SaaS solution. The vendor maintains its products FedRAMP Authorization, initially achieved on 30 May 2018 with Schellman Compliance LLC as Independent Assessor, package ID FR1724526654. The FedRAMP process is accepted under reciprocity agreements between FedRAMP and the US Government/Veterans Affairs.

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.*

VA has the sole ownership rights for all Intelliworx data. Below language is included in the Intelliworx contract.
VA INFORMATION CUSTODIAL LANGUAGE a. Information made available to the contractor or subcontractor by VA for the performance or administration of this contract or information developed by the contractor/subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1). b. VA information should not be co-mingled, if possible, with any other data on the contractors/subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct onsite inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements. c. Prior to termination or completion of this contract, contractor/ subcontractor must not destroy information received from VA, or gathered/ created by the contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf

of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its 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 termination of the contract. d. The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract. e. The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information. Also, the Intelliworx Service Level Agreement states: “All data stored in this environment is considered the customer’s data. In the case of multi-tenant systems, the customer owns the data associated with their organization as defined by the database’s foreign key structure.”

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.

Intelliworx collects no ancillary data.

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

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

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

The contact states: g. The contractor/subcontractor agrees to: (1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies: a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, contractors/subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The contractor's security control procedures must be equivalent to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be reviewed and approved by VA prior to implementation. b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

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).

Intelliworx does not utilize RPA.

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 they provided in this Privacy Impact Assessment is true and accurate.

HARASH KATYAL Digitally signed by HARASH KATYAL
Date: 2024.04.17 10:16:04 -04'00'

Privacy Officer, Harash Katyal

STEVE COSBY Digitally signed by STEVE COSBY
Date: 2024.04.17 10:26:37 -04'00'

Information System Security Officer, Steve Cosby

CHINO WALTERS Digitally signed by CHINO WALTERS
Date: 2024.04.18 07:37:42 -04'00'

Information System Owner, Chino L. Walters

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; screen shot of a website collection privacy notice).

System of records notice *Veterans Health Administration Human Capital Management (161VA10 / 88 FR 42005)*

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

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