Privacy Impact Assessment for the VA IT System called:

Region 6 - Workload Reporting and Productivity (WRAP) Assessing

Member Services (MS), Health Eligibility Center (HEC)

Veterans Health Administration (VHA)

Date PIA submitted for review:

September 26, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Shirley Hobson	Shirley.Hobson@va.gov	404-828-5337
Information System Security Officer (ISSO)	Howard Knight	Howard.Knight@va.gov	404-828-5340

	Name	E-mail	Phone Number
Information System Owner	Louise Rodebush	Louise.Rodebush@va.gov	216-849-0193

Abstract

The Workload Reporting and Productivity (WRAP) is a workload tracking tool owned by Veterans Affairs Office of Information Technology Field Program Office. WRAP is an in-house developed workload tracking tool that has been developed to meet Health Eligibility Center HEC customer requirements. The organization that operates the system is the HEC. Users that are authorized to use the system have the following access privileges: Supervisor (administrator) or WRAP User. All accounts are monitored and configured through Active directory.

Overview

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

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

The Workload Reporting and Productivity (WRAP) application is a locally developed tool that tracks Health Eligibility Center (HEC) Enrollment Eligibility Department (EED) and Income Verification Department (IVD) employees' workload and performance. VA employees use WRAP to manage HEC enrollment workflow processes. WRAP will use the Social Security Number (SSN), First Name, Middle Name, Last Name, and Veteran ID to identify Veterans throughout the eligibility and enrollment process and to complete updates once the Veteran is enrolled. Data will be secured via authenticating and limiting users who have access to it. Additionally, the application will be in a secure environment (behind the firewall) within the VA-HEC local area network. WRAP utilizes Hyper Text Transfer Protocol Secure (HTTPS), which means all communications between the user's browser and the web application are encrypted. WRAP is only accessible by internal employees with audit trails to safeguard the information. WRAP uses a server-to-server external read-only connection to Advanced Data Repository (ADR) database which is in Austin Information Technology Center (AITC) to obtain enrollment status by using Veteran's SSN as one of the identity traits. Enrollment applications and supporting documents will be scanned to the HEC imaging database and work flow items will be created and monitored by EED and IVD staff. These images can be viewed in WRAP but not stored.

- WRAP is a local application used by HEC internal and remote users.
- The application resides locally at the HEC-VHA on dedicated servers and administered by Atlanta Technology Center (ATC) staff.
- All processes to enroll, determine eligibility, update Veteran's information is performed outside of WRAP in the Enrollment System(ES) which is located in AITC.
- The HEC has the legal authority to use an SSN to enroll Veterans and conduct income verification. The requirement is that income be provided by the Veteran under Title 38 U.S.C. Section 5317.
- WRAP enables users to capture and report the following data:

  - the date EED received a request;
  - where the request came from;
  - method of communication to EED;
  - the Veteran associated with the request;
  - non-Veteran specific inquiries;
  - who the request or inquiry was assigned to within EED;
  - the date the transaction was assigned to staff;
  - status of the request;
  - date associated with the status of the request;
  - the remarks associated with the transaction.

- WRAP allows for easy management of User's workload by keeping them aware of workload assigned to them and its status.
- The last five years an average of 257064 Veterans' information was stored in WRAP. Veterans whose information is stored in the system over the years:

2005	53273
2006	87360
2007	80614
2008	77950
2009	91128
2010	123012
2011	157235
2012	150332
2013	223733
2014	196772
2015	204393
2016	215880

2017	274810
2018	272981
2019	225149
2020	210099
2021	300089
2022	277004

Primarily information is from patients requesting care as a Veteran of the U.S. Armed Forces. However, there are exceptions which are non-Veterans who may request care and their information is maintained in WRAP also. Exceptions are:

- *TRICARE* is the Department of Defense (DoD) regionally managed Healthcare program for service families. *TRICARE* Online may be used to make medical appointments, review medical claims, order prescription renewals or refills, and make enrollment changes. The system may also permit users to communicate electronically with health care providers, create or customize a *TRICARE* Online web page, and use the Personal Health Care Manager.
- Sharing Agreement: This is defined as resources sharing between the two departments encompassing a wide range of services, from the construction of joint medical facilities for use by VA/DoD beneficiaries to joint use of laboratory or laundry services. The purpose of the VA/DoD Healthcare Resources Sharing Program is to encourage the cost-effective use of Federal Healthcare resources by minimizing the duplication, and the under use of healthcare resources, while benefiting both VA and DoD beneficiaries.
- Allied Veteran Country: This is defined as the beneficiary's qualifying Allied Country. This data is shared with VistA. If an Allied country is selected, the beneficiary will be assigned an Eligibility Code of Allied Veteran. The Allied Veteran Country is required information for registration as an Allied Beneficiary. Authorized selections are (1) Canada or (2) United Kingdom (UK) Great (GRT) Britain / N. Ireland. Qualifying service with Poland and/or Czechoslovakia grants veterans' eligibility as a nonservice-connected beneficiary provided they meet the qualifications as outlined in the Allied Beneficiary Handbook.

- Qualifying Allied Beneficiaries are eligible for treatment for Service Connected (SC) conditions only and the Allied Country should authorize the care and reimburse VA. Allied Beneficiaries are individuals receiving a war pension or equivalent for service-related conditions or disabilities from a country who was allied or associated with the United States in World War I (except any nation which was an enemy of the United States during World War II), or inworld War II, with agreements requiring reimbursement (reciprocal agreements) with the United States (currently only England (UK. GRT Britain / N. Ireland) and Canada). If the Allied Beneficiaries served with Poland and/or Czechoslovakia and are in receipt of a VA monetary benefit from Great (GRT) Britain based on a SC condition, they can elect to be registered as an Allied Beneficiary and country of UK. GRT Britain / N. Ireland will be selected as the Allied Veteran Country. Allied Beneficiaries are eligible for treatment for SC conditions only and the Allied Country should be billed for their care. Poland and/or Czechoslovakia veterans cannot elect both Allied Veteran Status and nonservice-connected eligibility.

    - CHAMPVA: Civilian Health and Medical Program of the Uniformed Services or Veteran's Affairs (CHAMPVA) is an insurance program in which the VA shares the cost of covered health care services and supplies for active duty and retired career military persons, their dependents, and their survivors. The spouse or widow(er) and the children of a veteran who meet the criteria of CHAMPVA eligibility.

- Employee: This is an employee of the VAMC. The beneficiary is an employee of the VAMC or one of its associated sister facilities.
- Collateral of Veteran: Collateral of Veteran is a person related to or associated with a veteran receiving care from the VA. The beneficiary is seen by a professional member of the VA Health Care facility's staff either within the facility or at a site away from the facility for reasons relating to the veteran's clinical care. The beneficiary is not a veteran but is associated with a veteran through a specific program of care.
- Other Federal Agency: This is defined as another source for the beneficiary's rated SC disability. Examples might include any organization of the U.S. Government, such as Department of Defense, Veterans Administration, etc.

- The completion of this Privacy Impact Assessment will not result in any technology changes within HEC-VHA.
- The HEC-VHA is not in the process of modifying our system, therefore; the SORN modification will not be required at this time.
- The HEC-VHA does not use cloud technology currently.
- The HEC-VHA does occasionally have privacy violations that disclose veteran information to a third party. The Privacy Officer obtains credit monitoring and identity theft insurance protection for the veteran whose information was disclosed. Every attempt is made to insure the veterans of their privacy protection to avoid harming the reputation of the HEC-VHA and VHA.

The magnitude of potential harm if privacy related data is disclosed is high, due to the potential for identity theft. The reputation of the VA could be negatively impacted by a privacy related data disclosure.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

☒ Name
☒ Social Security Number
☒ Date of Birth
□ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
□ Personal Fax Number
☒ Personal Email Address
□ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
□ Financial Account Information
□ Health Insurance Beneficiary Numbers Account numbers
□ Certificate/License numbers
□ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
□ Current Medications
□ Previous Medical Records
□ Race/Ethnicity
□ Tax Identification Number
□ Medical Record Number
☒ Gender
□ Integration Control Number (ICN)
☒ Military History/Service Connection
□ Next of Kin
☒ Other Unique Identifying Information (list below)

- Place of birth
- Spouse's information – name, SSN, date of birth, date of marriage, address, phone number
- Child(ren)'s information – name, SSN, date of birth, date became dependent, relationship, disability, attending school
- Aid to child/spouse
- Gross annual income for each person listed on the form
- Previous calendar year deductible expenses
- Previous calendar year net worth
- Income Verification Department (IVD) case number

WRAP application only requests minimal information for processing of the workflow and when-ever possible personal identifiable information (PII) is not returned unless absolutely required by the business for performing functions.

WRAP will collect the following data elements in addition to the elements marked above to use when processing the workflow solution:

- Enrollment Status

Scanned image of VA Form 10-10EZ/EZR, and supporting correspondence

PII Mapping of Components

Workload Reporting and Productivity (WRAP) consists of three key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by WRAP and the reasons for the collection of the PII are in the table below.

PII Mapped to Components
Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
HECWRAP	**Yes**	**Yes**	Name, Social Security Number, Date of Birth, Zip, Code, Phone Number(s), Email Address	Veteran identity verification	Access to system is limited; access requires PIV; access to system and components is audited
File Server	**Yes**	**Yes**	Name, Social Security Number, Date of Birth, Zip, Code, Phone Number(s), Email Address	Veteran identity verification	Access to system is limited; access requires PIV; access to system and components is audited
Administrative Data Repository (ADR)	**Yes**	**Yes**	Name, Social Security Number, Date of Birth, Zip, Code,	Veteran identity verification	Access to system is limited; access requires PIV; access to system

			Phone Number(s), Email Address		and components is audited

1.2 What are the sources of the information in the system?

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

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The information is collected from the individual as part of an application for benefits or an update. The entities providing specific information include:

- Veterans
- Veterans Spouse
- VAMC's staff
- Veterans' representatives (POA)

WRAP does not collect any other information from a commercial aggregator or public websites. The solution is entirely within the VA-HEC environment without external connections.

1.3 How is the information collected?

Veteran Online application, Online Transaction and hard copy mailed/faxed applications utilize a directed questionnaire format to aid the Veteran in providing the information required by VA Form10-10EZ July 2013 (OMB Approved No. 2900-0091) and VA Form10-10EZR Feb 2011 (OMB Approved No. 2900-0091). In addition, Veteran Online Application (VOA) pre-populates some of the pre-existing data associated to the Veteran that already exists in the ES and Master Veteran Index (MVI) to help expedite the Veteran's form submission by reducing the time to re-enter the information.

Data for EED workflow is collected from the scanned Imaging System, Enrollment System, Veterans Health Information Systems and Technology Architecture (VistA), Veterans, Health Eligibility Center Alerts, and Health Eligibility Center staff members.

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

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

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

WRAP is dependent upon consistency checks in ES and ADR and relies on external systems for providing accurate data. The Veteran identity data is verified for accuracy by WRAP querying ADR for Veteran's SSN, last name, first name, and date of birth. All information being stored within WRAP is verified to be the correct type and format (for example: a telephone number will have the appropriate number of digits, SSN must be 9-digits, etc.). WRAP application does not currently interface with any other government agency for data matching.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

The HEC has the legal authority to use SSN to enroll veterans and conduct income verification. The requirement is that income be provided by the Veteran under Title 38 U.S.C. Section 5317.

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

Privacy Risk: There is a risk that Veterans' sensitive data could be viewed by unauthorized people.

Mitigation: WRAP uses authentication for access to the solutions. As a result, only authorized people will be able to view information related to their areas. Additionally, WRAP also supports the U.S. Government's initiative to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy.
Both DoD Common Access Cards (CAC) and Federal Information Processing Standard (FIPS) 201 Personal Identity Verification (PIV) cards are supported in WRAP.

WRAP provides a range of options for Single-Sign On:

- Windows Network Single Sign On
- Public Key Infrastructure (PKI) Single Sign On

WRAP application will ensure the proposed solution meets all VHA Security, Privacy and Identity Management requirements including VA Handbook 6500.

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.

Name: Used to identify the beneficiary and to send correspondence as necessary.
Social Security Number: Used to identify the Veteran in all VA systems and as a resource for verifying eligibility and enrollment within VA.
Date of Birth: Used to confirm Veteran identity.
Mailing Address: Used to mail correspondence to Veterans.
Zip Code: Used to identify location of Veteran to mail correspondence.
Phone Number: Used to communicate with Veteran
Email Address: Used to communicate with Veteran
Birth Sex: Used to confirm Veteran identity
Enrollment Status: Used to assist staff responsible for authorizing and coordinating VA care
Scanned image of VA Form10-10EZ/EZR: This is used by VA staff to initiate the eligibility and enrollment process as well as to update existing enrolled Veterans' records.
Place of birth: the city and state where the individual was born. DOB is an identifying trait and it's used to properly identify the correct Veteran to determine his or her eligibility for VA Health Benefits.
Military Service Information: branch of service, entry and discharge dates, discharge type: used to determine eligibility for medical benefits
Military History: All military information, i.e. Purple Heart recipient, former Prisoner of War (POW), Line of Duty determination, Combat Veteran, Southwest (SW) Asia service, Vietnam service, radiation exposure, radium treatments, 30 days service at Camp Lejeune: used to determine eligibility for medical benefits
Private Insurance, Medicare and Medicaid: VA needs to know whether the Veteran has secondary insurance for billing purposes. The information is collected during the enrollment process via the 1010EZ & 1010EZR forms for billing. Private insurance does not impact the Veterans' eligibility for VA Health Care.
Spouse's information: name, SSN, date of birth, date of marriage, address, phone number A spouse is considered a dependent and his or her information, financial data is used to determine whether the Veteran meets the Means Test threshold.
Child(ren)'s information: name, SSN, date of birth, date became dependent, relationship, disability, attending school Children are considered dependents and the Means Test threshold is impacted based upon the number of dependents. This information is a part of the financial assessment to determine Veterans' eligibility for VA Health Care.

Aid to child/spouse: This information is used as a part of the financial assessment and impacts the Means Test threshold. For example, if the Veteran has a special needs child or a child in college this information is deemed favorable during the financial assessment.
Gross annual income for each person listed on the form: used to determine eligibility for medical benefits
Previous calendar year deductible expenses: used to determine eligibility for medical benefits

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

Sensitive data elements are not analyzed by WRAP.

2.3 How is the information in the system secured?

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

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

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

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

Database storing WRAP data is encrypted. Users' connection to the system is encrypted using latest SSL/TLS protocols.

Access to system is limited; access requires PIV; access to system and components is
Audited.

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

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

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

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

<u>Principle of Use Limitation:</u> 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:

Access to WRAP is possible only by a WRAP administrator granting access. Access is granted on a need-to-know basis. HEC staff will need to complete and sign the VA Light Electronic Action Framework (LEAF) Access Request Form, obtain supervisor's signature for approval. The supervisor will verify the staff completed Privacy training, Cyber Security Training, and signed the Rules of Behavior by approving the LEAF Access Request Form. Access is only granted by the administrators when presented with LEAF Access Request Form signed by the user's supervisor and approved by the HEC EED/IVD department associate director.

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

All data listed in 1.1 will be retained in the WRAP Server Farm (scanned images) and ESR. In WRAP SQL database track who, what and when, but also from what and to what.

3.2 How long is information retained?

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

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

Per Records Control Schedule (RCS 005-1), hard copy documents are scanned into an electronic format and can be removed no more than 3 years of last date of service per Veteran. Hard copy records are managed/maintained for 30 days, at such time they are shredded. Electronic usage within

WRAP can be removed when eligibility has been verified and such information in WRAP has been entered the permanent Enrollment System. Time limitations can vary due to verification of enrollment. Any deletion, removal, etc. of information within the WRAP system will be documented through Privacy and Records Management Officers in conjunction with Information Technology and ATC groups but not any frequency greater than three years for tracking purposes.

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.

All records are maintained in accordance with the VA Office of Information & Technology (OI&T) Records Control Schedule (RCS 005-1), NARA and General Record Schedule (GRS) guidance. All records within the database are considered temporary as they are entered into WRAP, with the final process of migration into the Enrollment System.

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

All records found to have met Records Control Schedule (RCS 005-1) and NARA standards for removal from database or electronic format will follow those standards for removal from database/servers in the following manner.

All records for archiving will be placed on a CD or other electronic format submitted to Records Control Manager for archiving to Neosho, MS. This includes completion of archive request, in conjunction with Director, HEC signature, electronic request submitted through Archive database, listing of contents, e.g. date range, application, etc. then processed and shipped to Archive Center.

All hard copy shredding will be in accordance with the above and IRS requirements, Income Verification Only, as stated in above paragraph. Regardless of the record medium, all records are disposed of in accordance with the records retention standards approved by the Archivist of the United States, National Archives and Records Administration, and published in the VHA Records Control Schedule 10-1.

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

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

The WRAP Information System does not use PII for testing, research or training.

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.

Privacy Risk: The risk that Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) may be breached by insider threat increases the longer the information is retained.

Mitigation: All access connections are through a Windows Active Directory Accounting System. Insider threat is mitigated through mandated security vetting and security and awareness training. There is utilization of two factor authentication (PIV and pin sign on). This utilizes the Federal Government Security standards. Access to the database is on a limited basis and is terminated when any employee leaves the division and/or VA itself. All access is specific to person and division with only minimal access given based on need of the user. All database access is maintained in a secure environment, e.g. information is secured from national, network to user, behind fire walls and maximum protection of security. Information is retained in accordance to HEC, Records Control and General Records Schedules.

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*
Austin Information Technology Center (AITC) / Administrative Data Repository (ADR)	WRAP retrieve Veteran information from the Enrollment System at the AITC, as listed above in 1.1	Scanned images return from Veterans that potentially contain Federal Tax Information (FTI)/PII	Unidirectional only. Server to Server read- only connection to ADR database

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: The risk that Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) may be breached increases if information being shared within the Department is not secured.

Mitigation: WRAP application is accessible via Windows Authentication. This allows only authorized users to gain access to the information within the application regardless if users are within the same department, each user has a unique login username. The application is also configured to time-out (logout) any user session that is left un-attended thereby preventing unauthorized access to the data.

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

WRAP does not share information with any external organization, agencies, or IT systems.

Data Shared with External Organizations

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

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

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

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

Follow the format below:
Privacy Risk: As WRAP does not share data with any outside organizations, there are minimal to no privacy risks to the data collected, stored, and maintained in the system.

Mitigation: The key mitigation to any privacy risk related to external sharing of VA data from WRAP is that the system does not connect to or share with any external organizations or systems.

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.

Refer to this SORN 147VA10NF1 Enrollment and Eligibility Records—VA for WRAP does not provide direct notice to individuals upon collection of information, as HEC staff collects initial data from existing VA systems. However, notice is provided by the VA when a Veteran enrolls or re-enrolls for VA health benefits and completes either VA form 10-10EZ (Enrollment Application for Health Benefits) or VA form10-10EZR (Health Benefits Update Form).

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

WRAP does not provide Veterans with the direct opportunity to decline to provide information to the application. However, when enrolling for VA healthcare benefits, a Veteran does have the right to decline.

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

Once information is provided during enrollment and populated in the Enrollment System, WRAP uses the data to create work items and monitor status. As such, there is no opportunity to consent to uses of the data supplied to WRAP.

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

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

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

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

<u>Principle of Use Limitation:</u> 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: Because WRAP does not control the Veteran information collected, the Veteran information received by WRAP could change without proper public notice of collection and disposition of assumed information.

Mitigation: The VA mitigates this risk by ensuring that this PIA – which serves as notice that WRAP exists, the information it contains, and the procedures used to manage the information – is available online per the requirements of the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii). A review of the system is conducted annually, and a Privacy Threshold Analysis (PTA) updated with any changes to the system, data collected and disposition of the data.

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.

Records in WRAP should be covered under the Enrollment and Eligibility Records – VA (147VA10NF1) System of Records. Individuals seeking information regarding access to Enrollment and Eligibility Records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, Georgia 30329.

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.

Any veteran data that appears in WRAP cannot be changed because the data presented is pulled from the Enrollment System outside. WRAP is an employees' performance tracking system only. Any corrections to Veterans' data would be done at Enrollment System. Changes to the workflow are impacted within the WRAP system.

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.

Information in WRAP is validated against the Enrollment System and other verification databases and staff make updates in WRAP, if applicable. Also records in WRAP should be covered under the Enrollment and Eligibility Records – VA (14710NFA) System of Records. Individuals seeking information regarding amendments to Enrollment and Eligibility Records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, Georgia 30329. The appropriate supporting documentation should be provided.

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.

Records in WRAP should be covered under the Enrollment and Eligibility Records – VA (14710NFA) System of Records. Individuals seeking information regarding amendments to Enrollment and Eligibility Records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, Georgia 30329. The appropriate supporting documentation should be provided.

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 a Veteran could accidentally provide incorrect information to VA when enrolling for health benefits and that incorrect information could be used to determine case status.

Mitigation: WRAP is used to validate data; however, the data cannot be corrected in WRAP. It uses information provided by the Enrollment System for consistency checks. All processes to enroll, determine eligibility, and update Veterans' information are performed in the Enrollment System. However, Veterans do have the ability to update their enrollment information using VA form10-10EZR.

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.

User accounts are provided by the WRAP administrators – VA staff that has been verified by the supervisor through an access request process, who have taken the required training, and agreed to Rules of Behavior, will have access on a need to know basis. All users must be VA cleared.

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.

ATC contractors will have access to the system because the servers where the WRAP application resides are hosted by ATC. Access is required by the contractors for operations and maintenance but is limited by separation of duties. All our contracts are fixed rate contracts and do not require reviewing unless there's a need to validate contractor responsibilities or additional information is needed off the contract. If the contract has an option period, then it is reviewed prior to exercising the option. ATC Contractors have a proper background investigation and sign an NDA. Periodically, those are reviewed.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.
This question is related to privacy control AR-5, Privacy Awareness and Training.

All VA staff that has access to VA sensitive information must take the following training:

- Information Security Awareness and Rules of Behavior
- Privacy and HIPAA Training

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*

6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

1. The Security Plan Status: Approved
2. The Security Plan Status Date: 9/30/2020
3. The Authorization Status: Authorization to Operate (ATO)
4. The Authorization Date: 12/18/2020
5. The Authorization Termination Date: 12/17/2023
6. The Risk Review Completion Date: 12/17/2020
7. The FIPS 199 classification of the system; HIGH

Section 9 – Technology Usage

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

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

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

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

No, WRAP is using on-premises servers.

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

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

N/a

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

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

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

N/A

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

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

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

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

SHIRLEY HOBSON

Digitally signed by SHIRLEY HOBSON
Date: 2022.11.09 15:48:29 -06'00'

Privacy Officer, Shirley Hobson

Howard Knight 1508786

Digitally signed by Howard Knight 1508786
Date: 2022.11.10 08:21:38 -05'00'

Information System Security Officer, Howard Knight

Louise Rodebush 296012

Digitally signed by Louise Rodebush 296012
Date: 2022.11.10 09:16:43 -05'00'

Information System Owner, Louise Rodebush

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

VHA Notice of Privacy Practices

VHA Privacy and Release of Information