Privacy Impact Assessment for the VA IT System called:

IAM – Veterans Health Identification Card (VHIC)

Veterans Affairs Central Office (VACO)

ITOPS Infrastructure Operations (IO), Development, Security, and Operations (DevSecOps)

eMASS ID 2467

Date PIA submitted for review:

5/6/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer (PO)	Gina Siefert	gina.siefert@va.gov oitprivacy@va.gov	202-632-8430
Information System Security Officer (ISSO)	Lawanda Wells	Lawanda.wells@va.gov	(202) 632-7905
Information System Owner (ISSO)	Edward Merica	edward.merica@va.gov	512-326-6137

Abstract

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

IAM-Veterans Health Identification Card (VHIC) provides increased security for Veteran personal information for identification and check-in at VA appointments.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

VHIC's business purpose is to create a health card that provide the means for the VA to identify each person and provide said person the ability to check into appointments VA facilities.

Veteran Health Identification Card (VHIC) card is issued to Veterans who are enrolled in the VA health care system and is used for identification and check-in at VA appointments. VHIC provides increased security for Veteran personal information - no personally identifiable information is contained on the magnetic stripe or barcode; unique Member Identifier the Department of Defense assigns an electronic data interchange personal identifier (EDIPI) that allows VA to retrieve the Veterans health record.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

The system is VA Owned and VA Operated. The system's Data/Business/Information Owner is the Director of Infrastructure Operations (IO) Cybersecurity Management (ICSM)

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

The expected number of individuals whose information is stored in the system is over a million and the typical clients or affected individuals are Veterans.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☐	VA Employees
☐	Clinical Trainees
☐	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

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

Personal Identity and Authentication Information is used to ensure that all persons who are potentially entitled to receive any federal benefit are enumerated and identified so that Federal agencies can have reasonable assurance that they are paying or communicating with the right individuals. In the case of VHIC, the information used for identification and check-in at VA appointments and provides increased security for Veteran personal information.

E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

The information sharing that is conducted by the VHIC consists of operational data. This sharing type maintains records of user actions (i.e., authentication, authorization of access), security events, automated workflows, and various reporting analysis.

- Authorization Management Service references other components of the system to authorize the use of partner applications and veterans

- Compliance Auditing and Reporting collects audit records of action on the system (e.g. user logons) and provides reports of record metrics.

- Manages and correlates the ability to uniquely identify a person and the facilities where that person receives care is a key asset in the delivery of quality care System use resources through VA Enterprise Architecture.

F. Are the modules/subsystems only applicable if information is shared?

Yes.

G. Is the system operated in more than one site to include primary and secondary 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?

This system is operated at one site.

3. Legal Authority and System of Record Notices (SORN)

H. What is the citation of the legal authority?

Legal authorities are Title 38, United States Code, Section 501 and Title 38, U.S.C. Chapter 3, Section 210 (c) (1), Title 38 U.S.C. 7301, 5 U.S.C. 552a.and Executive order 9397.

I. What is the SORN?

- 79VA10/85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

Currently, the system is not in the process of being modified. This a new system that is seeking an accreditation. The applicable SORN that is associated with system does not require an amendment or revision currently.

4. System Changes

K. Will the business processes change due to the information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

K. Will the technology changes impact information collection and sharing?

☐ Yes
☒ No

if yes, <<ADD ANSWER HERE>>

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 Information 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
- ☒ **Full** Social Security Number
- ☐ **Partial** 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
- ☒ Sex
- ☒ Integrated Control Number (ICN)
- ☒ Military History/Service Connection
- ☐ Next of Kin
- ☒ Date of Death
- ☒ Business Email Address
- ☒ Electronic Data Interchange Personal Identifier (EDIPI)
- ☐ Other Data Elements (List Below)

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

Other PII/PHI data elements:

1.2 List 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?

The data from VHIC is derived from the VA-Master Person Index (VA MPI). The system checks accuracy against the stored credentials to provide access to VA/ DOD applications. User's information and PII accessed by VHIC comes from Credential Service Providers external to the system

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.

The IAM-VHIC system does not use data from a commercial aggregator nor public websites. The system has trusted internal and external connections in which data is derived.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

VHIC does not create new unique information nor provide reports for external distribution.

1.3 Methods of information collection
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?

The VHIC System integrates with IAM Single Sign-On Internal (IAM SSOi) to allow seamless access to the VHIC 4.32 application and integrates with Enrollment and VA MPI to obtain the proper Veteran information.

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?

Information is not collected on a form and/or is not subject to the Paperwork Reduction Act.

1.4 Information checks for accuracy, and 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.

VHIC receives information from VA-MPI, which is the authoritative source. VHIC does not collect the information on behalf of its users. The system checks accuracy against the stored credentials to provide access to VA/ DOD applications. User's information and PII accessed by VHIC comes from Credential Service Providers external to the system; it is externally collected and accessed.

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?

The system does not use a commercial aggregator to check for accuracy.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

This system is maintained under the legal authority of Title 38, USC, Section 501 and Section 7304. VHIC is not a System of Records and the PII received from the system is extracted from VA-MPI, which is a System of Record. The VA-MPI System of Record Notice (SORN) is Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10/85).

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.

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

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

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

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

Follow the format below when entering your risk assessment:

Privacy Risk:

Unauthorized Disclosure of Information – A data leak/break may result in the event of an individual (malicious) gaining access to VHIC system. This risk may lead to the exposure of sensitive information resulting in possible identify theft, social engineering, and fraud thus impacting the veteran.

Mitigation:

Authorization/Verification - This system is intended to be used by authorized individuals who currently exist record within the VA-MPI. Any individual who cannot be verified via the self-service portal will be denied access. Individuals who use the system have a a level of understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government intranet or Extranet (non-public) networks or systems.

Active Monitoring/Record Reconciliation - All transactions that occur on this system and all data transmitted through this system are subject to review. Anomalies that occurred are logged for analysis, a root cause identified that may/will result in resolution that can come in various methods (i.e., account deletion, password reset, verification change method, etc.).

Account Lockouts - Unauthorized attempts or acts to either (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, or (4) accrue resources for unauthorized use on this system are strictly prohibited. Activity is logged for investigation and accounts will require a possible password reset and/or account recreation.

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.

VHIC will take the information gathered from the VA-MPI and use the information to verify the individual (veteran) prior to listing any information pertain to the veteran's record. The information elements include Email (Work/Personal, Name, Integration Control Number, Sex, Date of Birth (DOB), Personal Mailing Address, EDIPI (DoD), SSN, Date of Death, and Military History/Service Connection.

PII/PHI Data Elements	Internal Use	External Use
Email (Work/Personal)	Assists in uniquely identifying the person's record.	Assists in uniquely identifying the person's record.
Name	Assists in uniquely identifying the person's record.	Assists in uniquely identifying the person's record.
Integration Control Number	Unique VA Identification (ID) number used to bring all separate SourceIDs together across the enterprise.	Unique VA Identification (ID) number used to bring all separate SourceIDs together across the enterprise.
Sex	Assists in uniquely identifying the person's record.	Assists in uniquely identifying the person's record.
Date of Birth (DOB)	Assists in uniquely identifying the person's record.	Assists in uniquely identifying the person's record.
Personal Mailing Address	Assists in uniquely identifying the person's record.	Assists in uniquely identifying the person's record.
EDIPI (DoD)	Assists in uniquely identifying the person's record.	Assists in uniquely identifying the person's record.
SSN	Assists in uniquely identifying the person's record.	Not used
Date of Death	VA indicator that the person could be deceased.	Not used
Military History/Service Connection	Assist in providing details of military schools attended, military courses completed, and military occupations held by the veteran.	Assist in providing details of military schools attended, military courses completed, and military occupations held by the veteran.

2.2 Describe the types of tools 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 IAM-VHIC systems has three tools that are utilized to perform analysis of data, performance anomalies, and overall health. The following list of tools and descriptions are:

- **CA Unified Infrastructure Management** (CA UIM) – The tool delivers availability, performance and service level management for heterogeneous IT networks. The solution automatically discovers network devices and interfaces and monitors device health and performance.

- **Oracle Enterprise Manager (OEM) -** The system management tool provides an integrated solution for managing Oracle products.

- **Splunk** – The enterprise tool conducts analysis in real-time, searching, monitoring, and analyzing machine-generated data. It collects and indexes data into a searchable index, enabling users to create graphs, reports, alerts, dashboards, and visualizations.

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

No 'new' data elements or information is created. There is no new data produced, rather a validation of existing provided data from VA-MPI sources.

2.3 How the information in the system is 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?

Data confidentiality and integrity is ensured via administrative, technical and physical controls. Physical access to the servers is restricted to authorized personnel in a data center at a facility with 24-hour security. Network access to servers is managed through firewalls. Access via the network requires authentication for both the application and servers.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

The social security number is masked, making the numerical entry unreadable

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

VHIC requires PIV and token access for application partner access and from the customer point of view requiring appropriate Credentialling Service Provider (CSP) privileges in order to maintain the systems that have SSN and PII data. Regarding the CSP access, the only SSN or PII that a customer would be transmitted are their own after the customer requests and approves.

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?

Criteria, procedures, controls, and responsibilities regarding access is documented in the User Manuals by role. Access does require manager approval and access to the system is being monitored. Access to specific identities is not being monitored currently but changes to identities are tracked, monitored, and recorded. The responsibility of assuring safeguards for the PII is shared between the business data owner and technical owner group per VA 6500 guidelines.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Yes. Criteria for the VHIC system is documented within policies, procedures, production operation manuals, and users guides. The documents are controlled artifacts residing in data repositories (i.e., GitHub), and a designated SharePoint folder directory,

2.4c Does access require manager approval?

Yes, access does require manager approval and access to the system shall be monitored

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

Security controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include requiring the Annual VA Rules of Behavior and Elevated Rules of Behavior training is completed for all

employees, volunteers, and contractors prior to access to the system. Additionally, audits are performed to ensure information is accessed and retrieved appropriately.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

The information system owner has the overall responsibility to ensure PII safeguards are in place for the IAM-VHIC system.

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*

The VHIC system does not retain information; the system verifies and authentication information already existing within the VA-MPI (Master Person Index).

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.

The VHIC system does not retain information; the system verifies and authentication information already existing within the VA-MPI (Master Person Index).

3.3 The retention schedule 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. Please work with the system VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

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

The VHIC system does not retain information; the system verifies and authentication information already existing within the VA-MPI (Master Person Index).

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

The VHIC system does not retain information; the system verifies and authentication information already existing within the VA-MPI (Master Person Index).

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.

Electronic data shall be eliminated, or transfer based on the guidance presented in VA Directive 6500 VA Cybersecurity Program. SPI data that is printed shall be discarded via shredding or placed in locked containers for processing by an approved third-party. Data must be anonymized (marked unrecognizable) to safeguard SPI from exposure. Electronic SPI data must follow the destruction practice as directed by e National Security Agency (NSA)/Central Security Service (CSS) Storage Device Declassification Manual, and NSA Evaluated Destruction Devices, available at www.nsa.gov.

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.

The system does not use PII data for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document in 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: *The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

Principle of Data Quality and Integrity: *The PIA should describe 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:

- Data Retention Longevity: Lengthy (infinite) data storage may lead to a security breach resulting in exposure of sensitive information to unknown individuals/parties.

Mitigation:

- Policy Enforcement: Develop and adopt data retention policy and procedures to oversee the storage of data for extended periods of time. The IAM-VHIC system is an internal system within the VA. The record retention guidelines adopted by the organization align to the National Archive and Records Administration (NARA). Additional, record retention requirements are also listed in VHA Directive 6300(1). Affairs (VA) policy and mandates of the National Archives and Records Administration (NARA

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a **IAM - Veterans Health Identification Card (VHIC)** consists of one key component (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **IAM - Veterans Health Identification Card (VHIC)** 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 3.9a 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
VIC (referring to VHIC - Veterans Health Identification Card)	Yes	Yes	• Email (Work/Personal) • Name • Integration Control Number (ICN) • Sex • Date of Birth (DOB) • Personal Mailing Address • EDIPI (DoD) • SSN • Date of Death • Military History/Service Connection	To authenticate veterans to VA Information systems	Data is encrypted

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Veterans Enrollment System (VES)	VES is the primary Veterans Affairs (VA) system used to manage VA health benefits.	• Personal Mailing Address • EDIPI (DoD) • SSN • Date of Death • Military History/Service Connection	HTTPS (Web Services)
VA Master Person Index (VA-MPI)	VA-MPI is the authority to the VA on person identity.	• Email (Work/Personal) • Name • Integration Control Number • Sex • Date of Birth (DOB) • Personal Mailing Address • EDIPI (DoD) • SSN • Date of Death	HTTPS (Web Services)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk:

Unauthorized Access: This risk may lead to viewing/editing content by an individual who is not authorized to do so. This type of activity may lead to data leak to parties who have not need to view data that is sensitive in nature.

Comprise of Security Posture: Other systems may not have the same level of classification when sharing information between two or systems. Systems of lower data classification could like process data that the system is not authorized to do.

Mitigation:

Provisioning user accounts: Utilize the approve provisioning procedure to grant access to user accounts that support, manage, process, and develop code signature. This process requires a request to be generated to request access, provide justification for the access, and

captures signatures (i.e., supervisor, group, information system owner) before access is granted.

Memorandum of Understanding/Agreements: Ensure agreements are in place between internal system are authorized/approved to share information.

Training/Awareness: Ensure employees complete annual privacy and security training requirements to enforce a level of understanding concerning data sharing, and the protection of sensitive information.

Adopt Critical Encryption Modules: Ensure encryption algorithms are in place to protect systems from a data breach and when sharing information. Enforce the use of multi-factor authentication (MFA) to secure systems that are sharing 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Government Print Office (GPO)	The information being shared is used to deliver (mail) correspondence to veterans and service members receiving benefits and services.	• Name • Integration Control Number (ICN) • Sex • Date of Birth (DOB) • Personal Mailing Address • EDIPI (DoD) • Military History/ Service Connection	GPO/VA MOU	SFTP Secure File Transport Protocol (SFTP)

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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:

Privacy Risk: The sharing of VA information with external parties has the risk of unintentional data disclosure of controlled information. This unintentional exposure of information may result in the data breach, identity theft, and social engineering of veterans/service member accounts.

Mitigation: The mitigation efforts that have been established to safeguard the integrity and confidentiality of data to minimize privacy risk includes but not limited to configuration/adoption of access control rules, security event logging/auditing, the application of encryption, and employee training and awareness.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

The Department of Veterans Affairs (DVA) provides notices that are accessible and available publicly. Individuals may view information collection practices adopted by the organization by in various ways. The DVA privacy policy is located via https://www.va.gov; by selecting on the policy and navigating to information collection practices, individuals may related content associated with data collection. Next, Department of Veteran Affairs - Veterans Health Administration Directive 1605.01 (VHA Directive 1605.01) Privacy and Release of Information that is publicly accessible via the web outlines information collections practices that are in place for individuals to review.

6.1b If notice was not provided, explain why.

A notice (banner) does appear as an individual attempts to gain access the VHIC system.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

Upon visiting the va.org website (AccessVA), individuals are presented with options to select a third-party CSP to gain access to the VHIC system. Upon selecting a CSP portal, a notification appears (each CSP has different banner) informing an individual that they will be leaving VA website and information that will be needed to access the VHIC

system. The notification banner provides details on the security of the website and privacy disclaimer can be found as well.

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.

Yes, if an individual does not wish to provide information within the system, he/she will not be granted access resulting in the inability to access his/her healthcare record, and/or view upcoming scheduled appointments. If an individual elects to continue to use the VHIC system, they will do so by vising the VA website (AccessVA) and select the VA partner web interface (i.e., DOD CAC, DS Logon, VA PIV card, ID.ME, Login.Gov) of choice to gain access.

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.

No. Individuals (veterans) who elect to use the VHIC system have an existing healthcare record within the VA. VHIC serves as an identification mechanism for veterans that are enrolled in the VA Healthcare system and supports efficiencies at VA medical facilities.

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

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

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

<u>Principle of Transparency:</u> This is referring to sufficient notice provided to the individual.

<u>Principle of Use Limitation:</u> The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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 is unaware that their information is being collected by the system.

Mitigation: The DVA sends out correspondence to ensure veterans understand their rights regarding the sharing of sensitive information with this system and its internal components. The VA provides notice to individuals before collection of information with publication in the Federal Registrar of the following SORN: 79VA10/85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA. As well as the public posting of this Privacy Impact Assessment (PIA) for the system. The VA ensures all public facing portals maintain accurate privacy content and artifacts regarding privacy disclosure and sharing of content.

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

The guidance provided in which an individual (veteran) may gain access to his/her information can be located with the publicly access 79VA10/85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA
https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

The procedures as noted within the SORN for accessing information is as follows:

> *''Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing…, or write, call or visit the VA facility location where they normally receive their care. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.''*

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)?

VHIC is not exempt from any 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?

IAM-VHIC, neither approves, nor grants, individuals with access to their data. Individuals seeking to gain access to his/her information may using online portals (i.e., MyHealtheVet, Veterans Health Information Exchange (VHIE), or AccessVA.

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.

As outlined in-SORN - 79VA10/85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA
https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

''Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.''

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.

The DVA does not directly notify veterans to update their information within VA systems. Individuals my submit requests to update service records utilizing processing forms that available or contact a DVA customer representative for assistance.

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 DVA website provide numerous avenues that notify individuals of the procedures for updating their information.

- Individuals seeking to make changes to their records may use VA Form 1010EZR.

- Individuals may also interface with VA Patient Advocates for guidance at facilities where the Veterans Identification Cards are issued. Individuals are also prompted to confirm information at time of VHIC application on the VA VHIC application website.

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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk:
Inaccurate Data: This risk presents the possibility of missed appointments with care provider who may not provide the services applicable to the healthcare needs of the veteran.

Incorrect Data Classification: This risk may lead to data breaches concerning unauthorized access to sensitive and restricted information. This risk may lead to other risk associated with reputational and legal.

Mitigation:

Notification Announcements: The DVA shall send out correspondence to ensure veterans understand the importance of updating health record. This action shall prevent a mismatch of data entered into the VHIC portal (AccessVA) as well as credential service providers (CSP) portals.

Verify System Security Categorization: IT professionals shall ensure that system is classified correctly to process data elements that is captured, processed, and stored.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

Individuals requiring access to the VHIC system must have a request submitted by the supervisor via the enterprise ticketing system. Once justification has been reviewed and approved, the access request is routed to the appropriate team for processing. Access to the system is granted based on the following conditions.

- The individual that receives access are responsible for creating user accounts that grant access to the system once all approvals have been approved by supervisor, system owner, and/or business owner.
- The individual is responsible for the development of coding that is used to managed metadata and software code that produces the output for requested actions.
- The individual is responsible for the maintenance and support of hardware technology as well as the computing platform in which the system is running upon.

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?

VHIC is an internal system within the VA. No external organizations are authorized to access and/or manage VA systems.

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.

The VHIC application is built to accommodate a specific set of pre-established user roles. During the provisioning process, the VHIC user will have a role assigned to them, which will determine what aspects of the VHIC application are available to them. The following roles are assigned within the VHIC system.

- VHIC Associate role shall be assigned to individuals responsible for processing a card request and resolving card request issues
- VHIC Supervisor role is allowed to submit a request for user access to the VHIC application. The supervisor has the ability to create a card request and have access to most available reports
- VHIC Administrator role is reserved for the VHIC Business (HEC) team members responsible for the creation and maintenance of all other VHIC accounts/roles.
- VHIC Technical Administrators (Tier 3) have the ability to create a card request and have access to all available reports
- The VHIC Auditor role shall be assigned to users with read-only access to the VHIC System. The individual does not have the ability to create a card request but does have access to all available reports.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

Yes, contractors assessing the VHIC system sign confidentiality agreements. This action is taken is executed by the contracting officer representative (COR) prior to gaining access to VA resources.

8.2a. Will VA contractors have access to the system and the PII?

Yes, VA contractors will have access to the system.

8.2b. What involvement will contractors have with the design and maintenance of the system?

Contractors with job roles/responsibilities assigned to the VHIC system will be responsible for code development and maintenance of hardware/software assets that listed for the system. Contractors

who are developed, will develop code to improve functionality and the user interface (UI) of the VHIC system. Maintenance contractors are required to update hardware system patches, update software applications to prevent/minimize service -level attacks, respond to incidents concerning the system, and the overall health of the system throughout its lifecycle.

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.

On an annual basis, all VA employees and contractors must complete VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and individuals with access to PHI must complete Privacy and HIPAA Training (VA 10203). These courses are automatically assigned via the TMS 2.0 system.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

1. *The Security Plan Status:* Has not been completed.
2. *The System Security Plan Status Date:* Has not been completed.
3. *The Authorization Status:* Has not been completed.
4. *The Authorization Date:* Has not been completed.
5. *The Authorization Termination Date:* Has not been completed.
6. *The Risk Review Completion Date:* Has not been completed.
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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 not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

Currently, the VHIC authorization and accreditation (A&A) package is in progress. The initial operating capability (IOC) date is February 28, 2026.

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. ***(Refer to question 1.8 of the PTA)***

Yes. VHIC is in the VAEC Microsoft MS Azure Government (MAG) environment.

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes. The VA maintains ownership of the data, and selects which services can process, store, and host data. The CSP does not access or use the data for any purpose without agreement from the VA. VA determines where the data will be stored, including the type of storage and geographic region of that storage. VA manages access to its data, and access to services and resources through users, groups, permissions, and credentials that are internally controlled. VA chooses the secured state of the data. The CSP provides encryption features that protect data in transit and at rest and provides VA with the option to manage their encryption keys. VA Enterprise Contract, NNG15SD22B VA118-17-F-2284 for Microsoft Commercial and 47QTCA22D003G for Microsoft Azure Government.

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.

The cloud service provider (CSP) – VAEC does no collect ancillary data. VA has full ownership over the data stored in the cloud.

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.

Yes, contracts that are in place with identified CSP (i.e., Microsoft Azure) outline security and privacy data requirements/principes. Additionally, DVA has full ownership of data stored in its cloud-computing environment (VAEC - Azure). VHIC is major application operating within VAEC.

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

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

The system does not currently use Robotics Process Automation (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.

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2025.06.24 08:31:40 -05'00'

Privacy Officer, Gina Siefert

LAWANDA WELLS Digitally signed by LAWANDA WELLS
Date: 2025.06.23 06:19:34 -04'00'

Information System Security Officer, Lawanda Wells

FRANKLIN MERICA Digitally signed by FRANKLIN MERICA
Date: 2025.06.23 07:12:27 -05'00'

Information System Owner, Edward Merica

APPENDIX A-6.1

VA.gov automatically collects certain information about your visit to VA.gov web pages. We limit the data collected to meet specific business needs and to protect your privacy. We may know what path(s) you took on our websites, but we don't know who you are. We do not use this information to identify you personally without your express consent and an authorized purpose.

We automatically collect and store the following information about your visit to the VA.gov website:

General log information. Examples of general log information include, but are not limited to: Internet domain (for example, "xcompany.com" or "yourschool.edu"); Internet Protocol (IP) address; operating system; the browser used to access our website; the date and time you accessed our site; and the pages that you visited.

Referral and statistical information where we have links to or from the site you visited. Such data may include aggregate data such as the number of offsite links occurring during a visit to a VA.gov web page. It may also include specific data, such as the identity of the site which you visited immediately before or after our site. We do not use such data to identify you personally.

We use the general log information to help us make VA.gov sites more useful to visitors. We use it to learn about how locations on our site are being used, what information is of most and least interest, and how we can enhance ease of use by ensuring our sites can interface with the types of technology our visitors use. We also use such statistics to tell us of any possible site performance problems. Except for oversight, law enforcement investigations, or protection of the VA information technology infrastructure as authorized by law, no other attempts are made to identify you or your usage habits.

General logs are used for no other purposes than the purposes described above, and are scheduled for regular destruction in accordance with General Records Schedules published by the National Archives and Records Administration (NARA) and agency record control schedule requirements.

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)