Privacy Impact Assessment for the VA IT System called:

VTSHS VetRide

Veterans Transportation Program
VHA Member Services

Date PIA submitted for review:
09/30/2022

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Shirley Hobson</td>
<td><a href="mailto:Shirley.Hobson@va.gov">Shirley.Hobson@va.gov</a></td>
<td>404-828-5337</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Jeramy Drake</td>
<td><a href="mailto:Jeramy.Drake@va.gov">Jeramy.Drake@va.gov</a></td>
<td>509-956-8865</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Johnathon Coble Harrison</td>
<td><a href="mailto:Johnathon.CobleHarrison@va.gov">Johnathon.CobleHarrison@va.gov</a></td>
<td>720-325-3675</td>
</tr>
</tbody>
</table>
Abstract

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

The VetRide Solution is a Transportation Management Solution that provides routing, scheduling, budget, ambulance run reporting, and data collection. The solution integrates Mobile Data Computers (MDC), VA transportation and administrative user face via web browser, connectivity to community transportation resources for coordination of scheduled rides, and a self-service solution for Veterans to request, check status, and get route information of rides. The solution is designed to meet demands of all users, in very high quantity, and meet or exceed all VA security standards.

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?

VetRide is a cloud hosted solution created to help manage the Veteran Transportation Program (VTP) program. VetRide received a one year ATO on February 10, 2022 and is hosted on Veteran Affairs Enterprise Cloud Amazon AWS (VAEC AWS) and consists of web portals for access and an android mobile application for communication and data transmissions. The VetRide Self Service Portal and Passenger Mobile Application is used by Veterans to request rides and check pre-arranged
ride statuses. The VetRide Admin Portal is used by VTS staff to manage the VTS program to ensure the transportation needs of our Veterans are properly addressed. The VetRide solution involves registering and establishing Veteran accounts, requesting trips for Veterans, scheduling trips to transportation runs, assigning transportation runs to vehicles, manage VTS program related data (i.e. drivers, devices, Points of Interest (POIs), sites, users, Community-Based Outpatient Clinics (CBOCs). The Android Mobile Data Computer (MDC) Application is used by drivers of the VTS program to login and receive routing schedules sent from the web portal to the MDC device. A driver’s schedule can have one or more runs, and a run can have one or more waypoints. The driver will proceed to each waypoint where Veterans will be picked up or dropped off Veteran. The driver will then swipe the Veteran’s Veterans Health Identification Card (VHIC), or manually enter the Veteran’s member ID and name to record the loading and unloading of a passenger. Additionally, a driver can send canned messages to the web portal to clarify schedule, routing, or passenger data. Finally, the VetRide solution will allow a driver to submit fuel and maintenance logs. Third Party Portal and Vendor Pass Mobile Application is used by VA contractors to approve and complete ride requests assigned from VetRide Admin Portal. VetRide is an enterprise-wide solution used by over 100 sites.

This system falls under the VA Mobile Application Environment (MAE) –VA, (173VA005OP2), Privacy Act System of Records, and defines the uses of the information. (https://www.oprm.va.gov/docs/Current_SORN_List_1_26_2022.pdf)

The completion of this PIA will not result in circumstances that requiring changes to business processes, and will not potentially result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

*The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.*
Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- Name
- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial 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)
- Service Connection (Percentage Only)
- Next of Kin
- Other Unique Identifying Information (list below)

Veteran’s Member ID
Veteran’s Special Needs (e.g., Wheelchair, Walker, Stretcher, Oxygen)
Veteran’s Companions (Name, Phone)
Vehicle Identification Number VIN
VA Assigned Driver’s License Number
Driver’s VA Assigned Phone Number
VA Employee Assigned Email
Employee Date of Birth (Optional)
Contractor’s Phone Number (Optional)
Veteran’s Medicare Number
Veteran’s Medicaid Number
Veteran’s Insurance Number

**PII Mapping of Components**

VetRide consists of 2 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VetRide 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

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Database</td>
<td>Yes</td>
<td>Yes</td>
<td>See section 1.1 for types of PII that are collected.</td>
<td>needed to properly schedule trips, manage budgets, and ambulance reports</td>
<td>Least Privileges, Encryption, Audit/Access Logs</td>
</tr>
<tr>
<td>Warehouse Database</td>
<td>No</td>
<td>Yes</td>
<td>See section 1.1 for types of PII that are collected.</td>
<td>Generation of reports</td>
<td>Least Privileges, Encryption, Audit/Access Logs</td>
</tr>
</tbody>
</table>

### Internal Database Connections

VetRide does not connect, receive, or share PII with another internal VA organization, IT system, website or application

<table>
<thead>
<tr>
<th>Server Name</th>
<th>Database Name that contains PII/PHI</th>
<th>Specifically list the PII/PHI Data Elements Sharing (Internally)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Internal Connections Table

<table>
<thead>
<tr>
<th>Internal Organization Name</th>
<th>IT System Name</th>
<th>Specifically list the Data Elements</th>
<th>Method of Transmission</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### 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.

Veteran information is entered by a member of the VTS staff through VetRide Admin web portal, or Veteran information entered by Paramedic through Ambulance Provider Portal

All information is stored to a database and is periodically copied/transformed to the data warehouse.

It is necessary to collect this data to verify requested appointments. VetRide provides Veterans the primary benefit of keeping their scheduled medical care appointments.

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is entered in the admin portal by the mobility manager or transportation coordinator
Information is entered in the Ambulance Provider Portal by the Paramedic.

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.

VTS staff will manually confirm all Veteran and trip information entered through Admin Portal. This is accomplished by using VetRide information (e.g., last 4 SSN and last name) and manually searching other VA applications (e.g., appointment information). There is no direct integration between VetRide and any other VA application. Information entered through Ambulance Provider Portal is verified by Paramedic Supervisor.

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

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.
This question is related to privacy control AP-1, Authority to Collect

Within VA, the legal authority to gather and use the SSN to verify veteran information is outlined in VA Handbook 6507.1 Section 2 subsection a(8).

Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:

The VetRide terms and conditions to be read and acknowledged by the VetRide Users, contains a Privacy Act “Routine Uses” section describing how the information will be used.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information
Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.
Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

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

**Principle of Minimization:** Is the information directly relevant and necessary to accomplish the specific purposes of the program?

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

**Principle of Data Quality and Integrity:** Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current? 

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

**Privacy Risk:** There is a risk that information attributed to the Veteran is not matched to the appropriate Veteran.

**Mitigation:** To mitigate the risk of incorrect information being attributed to a Veteran, both VA and Kevadiya (KVD) have implemented the following technologies, policies, and procedures: 1. Once the current VTS data is loaded to the VetRide system, KVD applies additional algorithms to identify bad matches, based on personal descriptors and identifiers. Additionally, the VTS staff will conduct an audit to validate that Veteran and Veteran data are properly matched. Veteran data stored in KVD’s databases are updated on a regular basis based on new registrations and changes submitted by Veterans and the updated information is also validated based on KVD’s algorithms and a VTS Staff audit. 2. If KVD or VTS staff All VetRide records at VA sites are protected from unauthorized access by systems and include external security, access control, and identification procedures. The Vetride system will be hosted on Veteran Affairs Enterprise Cloud Amazon AWS (VAEC AWS) cloud infrastructure.

Access to reports of data checks is restricted to staff with a need to know to perform their official duties. VetRide reports are transmitted to authorized agents of the federal government security programs, and once received by that agent become the responsibility of that agent. KVD and Veteran Transportation Service (VTS) transmit these reports using secure transfer methods and include appropriate security and privacy notices in VetRide instructions on the use and protection of these reports.

Information collected through Ambulance Provider Portal can only be entered by Paramedic, and the Paramedic supervisor verifies information entered.
Section 2. Uses of the Information

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

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

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

The program’s business purpose is to manage the VTS program. Information within the system such as Veteran information, trip information, vehicle information, etc. is needed to provide Veterans with transportation services especially for their access to medical care and to properly and accurately respond to agency directed inquiries and audits as well as congressional inquiries.

The records and information may be used for statistical analysis to produce various management, workload tracking and follow-up reports; to track and evaluate the ordering and delivery of transportation equipment, and services; the planning, distribution, and utilization of resources; the possession and use of equipment or supplies; the performance of equipment and employees. The data may also be used for such purposes as assisting in the scheduling of tours of duties and job assignments of employees; the registration of vehicles and the scheduling of vehicle maintenance; for audits, reviews and investigations conducted by staff of the health care facility, the Network Directors Office, VA Central Office, and the VA Office of Inspector General (OIG); for quality assurance audits, reviews, investigations, and inspections; and for law enforcement investigations.

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

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual’s existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.
A data warehouse is used to analyze data from the VetRide application. From the data warehouse the following reports can be generated.

- Productivity Report
- Trip Count Report
- Unique Veterans Report
- Vehicle Productivity Report
- Passenger Report
- Vehicle Report
- Facility Report
- Mobile Device Report
- Ad-Hoc Reports

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?

Data is encrypted 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?

Admin Portal collects last 4 SSN. Last 4 SSN is masked, and only accessible to certain roles. Ambulance Provider Portal collected SSN. SSN is marked, and only accessible to certain rules.

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

VetRide is a cloud hosted solution which stores data remotely. The data when stored and transmitted are both encrypted. VetRide mobile application provides certain PII and PHI information to the drivers on need-to-know basis. The Mobile data is also transmitted and stored with encryption. The data stored on Mobile device is not permanently stored. Once the trip data is flushed to the server, it is removed from the device.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. 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. 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.*

Privacy and security training is provided to all members of the project. If a user is found inappropriately using information from the VetRide application their account can be blocked, and the individual could, depending on the circumstances, be terminated.

All KVD and VA employees handling Veteran information have gone through the “Privacy and HIPAA Training” and “VA Privacy and Information Security Awareness and Rules of Behavior” Talent Management System (TMS) trainings and will receive annual refresher training as prompted and recorded by TMS.

This system falls under the VA Mobile Application Environment (MAE) – VA, (173VA005OP2), Privacy Act System of Records, and defines the uses of the information.

**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*

**Trip Information**
- Who was picked up
- Where they were pick up
- Where they were dropped off
- When did the trip occur
- How many miles were driven
- What vehicle was used

**Veteran Information**
- Name
- Phone
- SSN
- Primary Address
• Mailing Address
• Needs (Mobility Type etc.)
• Date of Birth
• Race/Ethnicity
• Gender
• Patient Medical History
• Patient Medication
• Patient Allergies
• Medicare Number
• Medicaid Number
• Insurance Number
• Patient Assessment
• Chief Compliant Anatomic Location
• Chief Compliant Organ System
• Treatments Performed at Sending Facility
• Medications Given by Ambulance Provider
• Procedures Performed by Ambulance Provider
• Vital Signs Obtained by Ambulance Provider

Vehicle Information
• License Plate
• VIN

Driver Information
• Name
• Phone
• Primary Address
• Date of Birth
• Driver’s License Number

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.

When managing and maintaining VA data and records, VetRide will follow the guidelines established in pursuant to NARA General Records Schedules GRS 3.2, item 030 and item 031. This document specifies how long records will be retained by the VA, if/when they will be transferred to a national records storage location, and the length of time the records will be stored.
at the national level. For greater details related to records retention at the Veterans’ Health Administration, please review RCS10-1

VetRide database information will be retained for the life of the project, and the server logs will be rotated on a periodic basis. In VetRide, even when you delete information, that information is just flagged as deleted and blocked from general viewing and is not actually deleted from the database. A system administrator will be responsible for writing and executing a database script to permanently delete any data based on guidance from the VTS staff.

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.

When managing and maintaining VA data and records, VetRide will follow the guidelines established in pursuant to NARA General Records Schedules GRS 3.2, item 030 and item 031.

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 VetRide SPI is stored in the database. Information from the application is never deleted by users, but rather marked to be disabled by setting a flag. If the request came from the VA requiring data to be deleted, KVD can write and execute a database script to do so. Upon request from VA, KVD will securely delete all digital data.

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.
Currently PII is not used for research, testing, or training. Testing and Training is conducted within a staging environment which contains fake / generated data.

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.

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that the information contained in the VetRide System will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

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

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure
The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?
NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.
Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information? This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

NOTE: At this time no information is shared with internal IT systems to/from VetRide

Data Shared with Internal Organizations

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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 sharing of data is necessary to ensure the Veteran is picked up and dropped off in a timely manner in order to meet their scheduled BA benefit appointments. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized individual during account registration, vehicle scheduling, passenger tracking, and dynamic routing.

**Mitigation:** The potential harm is mitigated by access control, configuration management, audit and accountability measures, personnel security, system and communication protection, awareness training, identification authentication, system information integrity, security assessment and authorization, incident response, risk assessment, planning, and maintenance.

All personnel accessing Veteran information must first have a successfully adjudicated background screening (SAC). This background check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history records. A background investigation is required commensurate with the individual’s duties.

Individual users are only given job position specific access to individually identifying data. Access to VetRide requires a username and password. Passwords must be changed every 90 days, or the user will be locked out of the system. All access to VA systems requires a multi-layer authentication. The individual must first authenticate through Windows Active Directory to access the VA network and will then have to authenticate with unique Access and Verify codes when accessing a specific system e.g., VistA. Each authentication process has an automatic lockout based on unsuccessful logon attempts. Additionally, the internal systems are time limited with session timeout after a designated period of inactivity.

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

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure
Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

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

Follow the format below:

**Privacy Risk:** Third party ride service contractor could share Veteran name, address, contact information, or the special instructions with non-approved entity.

**Mitigation:** All third party contractors must coordinate with the facility Mobility Manager and not with the VetRide Hosted Solution for any specific ride requests. This is a practice currently in place across VA.

**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.

Notice is provided to all VetRide users when they log into the system (see APPENDIX A). Veterans must acknowledge they have read and understood the VetRide terms and conditions (see APPENDIX B) every time they make a ride request within VetRide.

Veteran’s accounts that are moved over from existing VTS systems to VetRide are not automatically notified. VTS Staff must notify Veterans via a call or email of the VTS transportation system changes.
Finally, this Privacy Impact Assessment (PIA) also serves as notice of the VetRide system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs “after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.”

A notice was published in the Federal Register, Vol. 78, No. 215, Wednesday, November 6, 2013, for the VA Mobile Application Environment (MAE) – VA, (173VA005OP2), Privacy Act System of Records.

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

Individuals cannot opt out from providing information because system does not function without that information. If individuals opt out, system will not provide them service.

The Veterans’ Health Administration (VHA) as well as the VetRide system request only information necessary to provide transportation services to Veterans and other potential beneficiaries. While an individual may choose not to provide information to VetRide, this will prevent them from obtaining the necessary transportation services. Employees and VA contractors are also required to provide requested information to maintain employment or their contract with the VA.

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

Providing VetRide requested information is a voluntary act and by reading and acknowledging the terms and conditions, individuals consent to the use of the requested information for the sole purpose of transportation services. Individuals cannot consent to only a portion of required data since all required data is needed to properly schedule trips and manage the VTS program. The information is not used for any other purpose.
6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

**Principle of Transparency:** Has sufficient notice been provided to the individual?

**Principle of Use Limitation:** Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

**Privacy Risk:** There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the VetRide system prior to providing the requested information.

**Mitigation:** This risk is mitigated by providing the terms and conditions when Veterans submit a transportation request. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training.

Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

**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.

Veteran
There are several ways a Veteran or other beneficiary may access information about them. The Department of Veterans’ Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility’s Release of Information (ROI) office.

Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact their Contract Officer Representative to obtain information.

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.

Mobility Managers and Transportation Coordinators can edit and correct VetRide data based on a request from the Veteran. Additionally, a Veteran can log in and adjust their ride scheduling information. For other inaccurate or erroneous information, the corrective procedure begins with a Veteran requesting the records in question from Release of Information (ROI). The Veteran then crosses out the information they feel is inaccurate or erroneous from the records and writing in what the Veteran believes to be accurate. The request for amendment and correction is sent to the facility Privacy Office for processing. The documents are then forwarded to the practitioner who entered the data by the facility Privacy Officer. The practitioner either grants or denies the request. Once the practitioner has reviewed the requested amendment the document goes to the practitioner’s supervisor for review. The Veteran is notified of the decision via letter by the facility Privacy Officer. The goal is to complete any evaluation and determination within 30 days.

Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative to correct inaccurate or erroneous information upon request.
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.

Veterans are informed of the amendment process by many resources to include the terms and conditions which states:

**Right to Request Amendment of VetRide Information.**

You have the right to request an amendment (correction) to your VetRide information if you believe it is incomplete, inaccurate, untimely, or unrelated to your VA transportation needs. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Mobility Manager at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:
- File an appeal
- File a “Statement of Disagreement”
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Information can also be obtained by contacting the facility ROI office.

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 ensure data accuracy.

An individual can call and request a Mobility Manager or Transportation Coordinator to make changes to their personal information. For all other situations, Veterans and other individuals are encouraged to use the formal redress procedures discussed above to request edits to their VetRide records and other personal records retained about them.

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 may not be familiar with how to obtain access to their records or how to request corrections to their records.

**Mitigation:** As discussed in question 7.3, the terms and conditions, which every Veteran reads and acknowledges prior to receiving VA transportation services, discusses the process for requesting an amendment to one’s records. The VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their medical records and other records containing personal information.

**Section 8. Technical Access and Security**

The following questions are intended to describe technical safeguards and security measures.

**8.1 What procedures are in place to determine which users may access the system, and are they documented?**

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

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

Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.
This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

System Security Plan (SSP) outlines detailed access control requirements for the VetRide system.

Access to VetRide working and storage areas is restricted to VA employees and contractors who must complete both the HIPAA and Information Security training. Specified access is granted based on the employee’s functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information Security Officer (ISO), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

VetRide access is requested using a VA Form 9957. This form will be completed and signed by the requester and their supervisor. Once signed it will be forwarded to a VTS Regional Coordinator who will confirm the information provided in the form. After all the information has been confirmed, the VTS Regional Coordinator will then grant, per the VA Form 9957, access to the specific facility’s database.

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.

Contractor has a Business Associate Agreement (BAA)

Kevadiya who is a VA Contractor, primarily responsible for the design and maintenance of VetRide, and are involved in most aspects of design and maintenance. Kevadiya is providing system administration to system which required access approval through VA. Kevadiya System Administrators requires privileged access to perform their roles and responsibilities of administrating the VetRide System. Privileged accessed users can access PII.

Will VA contractors have access to the system and the PII? Yes

If yes, what involvement will contractors have with the design and maintenance of the system? VA Contractors is primarily responsible for the design and maintenance of VetRide and are
involved in most aspects of design and maintenance. Engineers and Developers have elevated access through ePAS for the VAEC.

Describe the necessity of the access provided to contractors to the system and whether clearance is required -- Contractors are providing system administration to system which requires Contractors to have access approved through VA.

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. VA Contractors requires privileged access to perform their roles and responsibilities of administrating the VetRide System. Privileged accessed users can access PII.

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 KVD and VA employees handling Veteran information will complete “Privacy and HIPAA Training” and “VA Privacy and Information Security Awareness and Rules of Behavior” TMS trainings. Individuals must also have a personal identification verification (PIV) badge reflecting they have a favorably adjudicated SAC and either a scheduled or favorably adjudicated background investigation at least at the National Agency Check with Inquiries (NACI)/Tier 1.

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 – 11-17-2021
3. The Authorization Status - Authorization to Operate (ATO)
4. The Authorization Date – 02-10-2022
5. The Authorization Termination Date – 02-10-2023
6. The Risk Review Completion Date – 01-20-2022
7. The FIPS 199 classification of the system - MODERATE

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.

VA Enterprise Cloud (VAEC) AWS

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.

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.

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.

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).
## Section 10. References

### Summary of Privacy Controls by Family

<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td><strong>Authority and Purpose</strong></td>
</tr>
<tr>
<td>AP-1</td>
<td>Authority to Collect</td>
</tr>
<tr>
<td>AP-2</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>AR</td>
<td><strong>Accountability, Audit, and Risk Management</strong></td>
</tr>
<tr>
<td>AR-1</td>
<td>Governance and Privacy Program</td>
</tr>
<tr>
<td>AR-2</td>
<td>Privacy Impact and Risk Assessment</td>
</tr>
<tr>
<td>AR-3</td>
<td>Privacy Requirements for Contractors and Service Providers</td>
</tr>
<tr>
<td>AR-4</td>
<td>Privacy Monitoring and Auditing</td>
</tr>
<tr>
<td>AR-5</td>
<td>Privacy Awareness and Training</td>
</tr>
<tr>
<td>AR-7</td>
<td>Privacy-Enhanced System Design and Development</td>
</tr>
<tr>
<td>AR-8</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>DI</td>
<td><strong>Data Quality and Integrity</strong></td>
</tr>
<tr>
<td>DI-1</td>
<td>Data Quality</td>
</tr>
<tr>
<td>DI-2</td>
<td>Data Integrity and Data Integrity Board</td>
</tr>
<tr>
<td>DM</td>
<td><strong>Data Minimization and Retention</strong></td>
</tr>
<tr>
<td>DM-1</td>
<td>Minimization of Personally Identifiable Information</td>
</tr>
<tr>
<td>DM-2</td>
<td>Data Retention and Disposal</td>
</tr>
<tr>
<td>DM-3</td>
<td>Minimization of PII Used in Testing, Training, and Research</td>
</tr>
<tr>
<td>IP</td>
<td><strong>Individual Participation and Redress</strong></td>
</tr>
<tr>
<td>IP-1</td>
<td>Consent</td>
</tr>
<tr>
<td>IP-2</td>
<td>Individual Access</td>
</tr>
<tr>
<td>IP-3</td>
<td>Redress</td>
</tr>
<tr>
<td>IP-4</td>
<td>Complaint Management</td>
</tr>
<tr>
<td>SE</td>
<td><strong>Security</strong></td>
</tr>
<tr>
<td>SE-1</td>
<td>Inventory of Personally Identifiable Information</td>
</tr>
<tr>
<td>SE-2</td>
<td>Privacy Incident Response</td>
</tr>
<tr>
<td>TR</td>
<td><strong>Transparency</strong></td>
</tr>
<tr>
<td>TR-1</td>
<td>Privacy Notice</td>
</tr>
<tr>
<td>TR-2</td>
<td>System of Records Notices and Privacy Act Statements</td>
</tr>
<tr>
<td>TR-3</td>
<td>Dissemination of Privacy Program Information</td>
</tr>
<tr>
<td>UL</td>
<td><strong>Use Limitation</strong></td>
</tr>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
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: 2022.11.17 11:26:27 -06'00'

Privacy Officer, Shirley Hobson

JERAMY A. DRAKE 505947  
Digitally signed by JERAMY A. DRAKE 505947  
Date: 2022.11.29 12:32:47 -08'00'

Information Systems Security Officer, Jeramy Drake

JOHNATHON COBLE HARRISON  
Digitally signed by JOHNATHON COBLE HARRISON  
Date: 2022.11.29 13:00:48 -07'00'

Information System Owner, Johnathon Coble Harrison
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).

VetRide 2.0 (va.gov)

A notice was published in the Federal Register, Vol. 78, No. 215, Wednesday, November 6, 2013, for the VA Mobile Application Environment (MAE) – VA, (173VA005OP2), Privacy Act System of Records.
https://www.oprm.va.gov/docs/Current_SORN_List_1_26_2022.pdf

APPENDIX B
This U.S government system is intended to be used by [authorized VA network users] for viewing and retrieving information only, except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA. All use is considered to be with an 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. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms. 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. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties.