Privacy Impact Assessment for the VA IT System called:

My HealtheVet (Cloud) Assessing (MHV)

Veterans' Health Administration (VHA)

Enterprise Product Management Office (EPMO) eMASS ID 884

Date PIA submitted for review:

12/04/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Margaret L. (Peggy) Pugh Backup: Phillip Cauthers	margaret.pugh@va.gov Phillip.cauthers@va.gov	202-731-6843 503-721-1037
Information System Security Officer (ISSO)	Joseph W. Decoteau Backup: Leigh Zirbel	Joseph.Decoteau@va.gov Leigh.Zirbel@va.gov	802-624-2480 605-940-1310
Information System Owner	Sean Good	Sean.Good@va.gov	520-574-2173

Abstract

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

My HealtheVet (Cloud) Assessing" (MHV) is a web-based personal health record system that provides Veterans with information and tools that they can use to increase their knowledge about health conditions, foster better communication with their care providers, and improve their own health. With MHV, Veterans can take a more proactive approach to managing their health and utilizing VA health services and benefits.

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?*

The purpose of the MHV system is to provide a web-based application for Veterans, their families, and care providers to access health resources in an online environment. It improves Veteran health care by providing easy access to health information, online resources, and facilitates patient/health care provider interactions. MHV gives the Veteran access to VA benefits, special programs, and health information and services. It also provides the Veteran web-based tools to increase their knowledge about health conditions, manage their health records, and communicate with health care providers. With MHV, Veterans can take a more proactive approach to managing their health and utilizing VA health services and benefits.

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.*

VAEC Amazon, VA Owned and non-VA Operated IS.

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?*

As of December 2024, the number of Veterans who have information stored in the MHV system is over 5.5 million. The system has the capacity to support up to 20,000 concurrent connections and is designed to be scalable up to 100,000 concurrent connections. The MHV application serves Veterans: persons who served in the U.S. military, naval, or air service and now seek healthcare services through VA.

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?*

The MHV application allows Veteran's access to their Electronic Health Record (EHR), VA benefits, special programs, and health information and services.

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

MHV consists of multiple modules that can provide the Veteran with imaging data such as labs and allergy results, health summary reports, medications list, primary care provider information, appointments (various appointment types), immunizations, and other health related information.

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

No, the modules/subsystems are always applicable regardless of whether the information is shared or not.

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?*

The MHV web portal is operated across the country in VA facilities and by Veterans. It operates in compliance with privacy controls applicable to systems with Personally Identifying Information (PII) and Protected Health Information (PHI) being stored, transmitted, and processed. Privacy controls are documented in the MHV System Security Plan (SSP). Controls are also enacted for MHV in accordance with HIPAA Business Associate Agreement (BAA) policies and procedures. MHV handles and retains system information in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and operational requirements. The release of privacy-related data by accident or malicious intent would have zero, minor or moderate effects, based on protection controls such as those dealing with authentication, encryption, and firewall mechanisms.

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

H. What is the citation of the legal authority?

130VA10/89 FR 13806 - The collection of information as defined within the MHV Administrative Records VA 130VA10P2, Federal Register 13806 / Vol. 89, No. 37 / Friday, February 23, 2024, is based upon the Privacy Act of 1974, 5 U.S.C. 552a(e). VA 6508 is the directive which outlines the PIA requirement for every System/Application/ Program. The legal authority to operate the system is Title 38, United States Code, §501 and Executive Order 9397.

I. What is the SORN?

SORN Title: My HealtheVet Administrative Records-VA
SORN Number: 130VA10
https://www.govinfo.gov/content/pkg/FR-2024-02-23/pdf/2024-03715.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.

No

4. System Changes

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

☐ *Yes*
☒ *No*
if yes,

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

☐ *Yes*
☒ *No*
if yes,

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:

- All patient demographic updates sent from MPI to MHV
- Allergies
- Appointments
- ATTACHMENT_ID
- CMOP Tracking Number, CMOP Date Shipped, CMOP Carrier, Carrier Tracking Number
- DATE PROCESSED (Last Refill Process Date)
- DATE PROCESSED (MHV Refill Request Status Date)
- Date/timestamp
- Dispense Date
- Division Name
- Drug Name (Medication Name)
- Drug schedule
- Electronic Data Interchange Personal Identifier (EDIPI) from Department of Defense
- SAML Single Logout (SLO)
- SAML Single Sign On (SSO)
- SENDER_ID • SENDER_NAME
- SENDER_TYPE
- SENT_DATE
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Facility Phone Number
- Internal Entry Number (IEN)
- Labs (Chemistry/Hematology)
- LOGIN DATE (i.e., Last Refill Request Date)
- MHV Account Info
- MHV Identification (ID)
- MHV User ID
- Millennium Patient ID
- National Drug Code (NDC)
- Number of RX in Package
- Placer Order Number
- Prescription Number
- RESULT (MHV Refill Request Status)
- Unique Index
- USER_ID
- Users' Authentication Credentials
- VAMC Tracking Number
- Provider
- Trade Name
- Session information

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?

Individuals that provide the documented PHI/PII to the systems include Providers, VA staff, Veterans, caregivers, and beneficiaries who access MHV systems through the MHV National, Admin or SM Portal.

MHV users can store self-entered information relevant to their health and download/transmit that information via the MHV National Portal's Blue Button tools.

Clinicians and support personnel are granted access, based on a need to know/least privilege, to provide administrative support or treatment to the Veteran.

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.

Information is not collected from sources other than the Veteran, caregiver, provider or VA staff. MHV Portals do not use any commercial aggregators.

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

- HDR-Pathways both receive patient data, such as lab and allergy data, which is loaded into the user's Personal Health Record (PHR) for the purpose of displaying information within the web application and creating PHR summary reports that can be taken to external provider appointments.

- Veteran Benefits Handbook (VBH) is an interface through which data is sent electronically for the purpose of providing information about VA healthcare benefits the Veteran may be able to receive, such as medications or dental care data.

- Veteran Health Information Exchange (VHIE) is an interface through which MHV retrieves data such as the Health Summary and sends that CCD data to physicians outside of the VA network.

- VistA Interface Adapter (VIA) is an interface through which data is loaded into the user's PHR for the purpose of displaying the data within the MHV application and creating PHR summary reports that can be saved and taken to an external provider appointment.

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?

MHV collects PII/PHI directly from the individual or from the individual's legal representative whenever possible, which allows for better confirmation of the accuracy, relevance, timeliness, and completeness of the information.

MHV ensures the validity of information collected by the Veteran or third party (such as a family member) is accurate by obtaining acceptable forms of identification and/or supporting documentation.

PII and PHI is reviewed for accuracy as it is collected and utilized to care for Veterans. Once the information is collected, it is entered into the national ID management system, which further verifies accuracy of Veteran's PII.

To ensure that collected information is correct and up to date, MHV asks individuals to confirm the accuracy of the information that was entered in the system and to update them with any new information before their visit is over.

Information from users comes from either functionality exposed through one of our portal systems or services provided via APIs.

All information is collected /exchanged over secure protocols (HTTPS) using authenticated sessions.

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?

MHV information is not collected on a form.

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.

MHV collects PII/PHI directly from the individual or from the individual's legal representative whenever possible, which allows for better confirmation of the accuracy, relevance, timeliness, and completeness of the information.

MHV ensures the validity of information collected by the Veteran or third party (such as a family member) is accurate by obtaining acceptable forms of identification and/or supporting documentation.

PII and PHI is reviewed for accuracy as it is collected and utilized to care for Veterans. Once the information is collected, it is entered into the national ID management system, which further verifies accuracy of Veteran's PII.

To ensure that collected information is correct and up to date, MHV asks individuals to confirm the accuracy of the information that was entered in the system and to update them with any new information before their visit is over. Information from users comes from either functionality exposed through one of our portal systems or services provided via APIs. All information is collected /exchanged over secure protocols (HTTPS) using authenticated sessions

To ensure Veterans receive appropriate services and to protect privacy, system staff are responsible for authenticating the identity of Veterans and/or dependents accessing VA services by requesting one Primary Identification Document (state issue driver's license, passport, Veteran Identification Card, etc.). A Healthcare Portal (i.e., My HealtheVet (Cloud) Assessing (MHV) etc.) enrollment process supports verifying a subject's identity before allowing access to the application for increased authentication.

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 MHV system does not check for accuracy by accessing a commercial aggregator.

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

VA 6508 is the directive which outlines the PIA requirement for every system/application/ program.

The collection of information as defined within the MHV Administrative Records—VA 130VA10, located at: *https://www.govinfo.gov/content/pkg/FR-2024-02-23/pdf/2024-03715.pdf* as set forth in the Federal Register 193 FR 59991, is based upon the Privacy Act of 1974, 5 U.S.C. 552a(e). The authority for maintenance of the system is Title 38, United States Code, §501.

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

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

Principle of Purpose Specification: 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: MHV collects Personally Identifiable Information (PII) and Personal Health Information (PHI). If this information were to be breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: VA is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and help the affected parties so that they may find the help they need to get through their crisis. MHV employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These security measures include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA Directives.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name (First, Last)	Veteran identification used for display, verification, and reporting purposes	Veteran identification used for display, verification, and reporting purposes
MHV Account Info	JSON data that includes account type and available service information	JSON data that includes account type and available service information
Millennium Patient ID	Oracle Health identification used for display, verification, and reporting purposes	Oracle Health identification used for display, verification, and reporting purposes
Sex	Veteran identification used for display, verification, and reporting purposes	Veteran identification used for display, verification, and reporting purposes
Social Security Number	Veteran Identity Trait used for linking MHV user to Master Person Index (MPI) Veteran	Veteran Identity Trait used for linking MHV user to Master Person Index (MPI) Veteran
Date of Birth	Veteran Identity Trait used for linking MHV user to MPI Veteran	Veteran Identity Trait used for linking MHV user to MPI Veteran

PII/PHI Data Element	Internal Use	External Use
Personal Mailing Address	Veteran Identity Trait used for linking MHV user to MPI Veteran	Veteran Identity Trait used for linking MHV user to MPI Veteran
Personal Fax Number	May be provided by user as a means for contact (not required)	May be provided by user as a means for contact (not required)
Personal Email Address	May be provided by user as a means for contact and may be used for system notifications (not required)	May be provided by user as a means for contact and may be used for system notifications (not required)
Emergency Contact	May be provided by user as a means for contact in case of emergency (not required)	May be provided by user as a means for contact in case of emergency (not required)
Emergency Contact Information (Name, Phone Number, etc. of a different individual)	May be provided by user as a means for contact in case of emergency (not required)	May be provided by user as a means for contact in case of emergency (not required)
Medications	Supports Veterans' ability to review/ report on medications they are currently taking or have taken in the past, as well as provides a means for Veterans refilling a prescription to track the refill as it is being shipped to them.	Supports Veterans' ability to review/ report on medications they are currently taking or have taken in the past, as well as provides a means for Veterans refilling a prescription to track the refill as it is being shipped to them.
Medical Record	Supports the Veteran in obtaining their VA health information	Supports the Veteran in obtaining their VA health information
ICN	VA unique identifier for the user where one exists; used by the system only for correlation of information from various sources (e.g., MHV, VistA, CVIX, HDR, etc.); not exposed to the end user	VA unique identifier for the user where one exists; used by the system only for correlation of information from various sources (e.g., MHV, VistA, CVIX, HDR, etc.); not exposed to the end user
Previous Medical Record	Supports the Veteran in obtaining their VA health information.	Supports the Veteran in obtaining their VA health information.
MHV User ID MHV Identification (ID)	Unique identifier for User within the system (correlated in the MPI against the 200MH station number)	Unique identifier for User within the system (correlated in the MPI against the 200MH station number)
Prescription Number	Unique identifier for Prescription, original, refill and partial refills	Unique identifier for Prescription, original, refill and partial refills
Internal Entry Number (IEN)	MHV Database Identifier used for identifying prescriptions.	MHV Database Identifier used for identifying prescriptions.

PII/PHI Data Element	Internal Use	External Use
Drug Name (Medication Name)	Drug Name- aka Medication name in the MHV Database used with the Title Card in va.gov meds list (includes name, potency, and form)	Drug Name- aka Medication name in the MHV Database used with the Title Card in va.gov meds list (includes name, potency, and form)
Patient demographic updates sent from MPI to MHV	Used for identifying and verifying identity	Used for identifying and verifying identity
Allergies	Used by Medical Records API connection to Oracle Health	Used by Medical Records API connection to Oracle Health
Appointments	Used to track patient appointments information	Used to track patient appointments information
ATTACHMENT_ID	Used in Secure Messaging, a Number that maps to attachment ID	Used in Secure Messaging, a Number that maps to attachment ID
CMOP Tracking Number, CMOP Date Shipped, CMOP Carrier, Carrier Tracking Number	Tracking of prescriptions with CMOP- provides information about the prescriptions being sent or transmitted to CMOP or mailed by CMOP	Tracking of prescriptions with CMOP- provides information about the prescriptions being sent or transmitted to CMOP or mailed by CMOP
DATE PROCESSED (Last Refill Process Date)	This is the date the pharmacy processed the refill request.	This is the date the pharmacy processed the refill request.
DATE PROCESSED (MHV Refill Request Status Date)	MHV_STATUS_DATE only RF source/indexes as this is the date the pharmacy processed the refill request.	MHV_STATUS_DATE only RF source/indexes as this is the date the pharmacy processed the refill request.
RESULT (MHV Refill Request Status)	The result of the pharmacy staff processing the refill request.	The result of the pharmacy staff processing the refill request.
Division Name	Used for VistA to 'pull' a refill from another VAMC and fill it.	Used for VistA to 'pull' a refill from another VAMC and fill it.
Date/timestamp	Tracks when pharmacy processed medication	Tracks when pharmacy processed medication
Placer Order Number	Tracks Pharmacy order numbers	Tracks Pharmacy order numbers
Dispense Date	Tracks when pharmacy dispense medication	Tracks when pharmacy dispense medication
Electronic Data Interchange Personal Identifier (EDIPI) from Department of Defense	Used to associate records with an account with a specific number in the United States Department of Defense's Defense Enrollment and Eligibility Reporting System (DEERS) database	Used to associate records with an account with a specific number in the United States Department of Defense's Defense Enrollment and Eligibility Reporting System (DEERS) database
Facility Phone Number	Tracks which phone number of the Outpatient Pharmacy filled the prescription.	Tracks which phone number of the Outpatient Pharmacy filled the prescription.
LOGIN DATE (i.e., Last Refill Request Date)	Used to track the date MHV placed the refill request.	Used to track the date MHV placed the refill request.

PII/PHI Data Element	Internal Use	External Use
NDC	Sent from MHV database to perform refills used for every refill record.	Sent from MHV database to perform refills used for every refill record.
Number of RX in Package	Identifies number of RX in packages sent from CMOP	Identifies number of RX in packages sent from CMOP
VAMC Tracking Number	This field is used to indicate which fill activity took place.	This field is used to indicate which fill activity took place.
Trade Name	Used in Medication refills	Used in Medication refills
SAML Single Logout (SLO) SAML Single Sign On (SSO)	Used by MHV to authenticate users against MHV systems, Personal Identification Verification (PIV) card or Active Directory (AD) to provide the ability to seamlessly authenticate between systems	Used by MHV to authenticate users against MHV systems, Personal Identification Verification (PIV) card or Active Directory (AD) to provide the ability to seamlessly authenticate between systems
USER_ID	Used in login credential as a means for verification, and authentication of user access	Used in login credential as a means for verification, and authentication of user access
Users' Authentication Credentials	Used in login credential as a means for verification, and authentication of user access	Used in login credential as a means for verification, and authentication of user access
Provider	Veteran identification used for display, verification, and reporting purposes	Veteran identification used for display, verification, and reporting purposes
Unique Index	Refer to Source (e.g., RX = NULL for this value	Refer to Source (e.g., RX = NULL for this value
Session Info	Used with Iris/Newway/ Rightnow services	Used with Iris/Newway /Righnow services
SENDER_ID SENDER_NAME SENDER_TYPE SENT_DATE	Used to identify individuals who use and send Secure messages, patient to provider through DAS SPOE FHIR	Used to identify individuals who use and send Secure messages, patient to provider through DAS SPOE FHIR
Labs Chemistry/ Hematology	Tracking of information about tests that are routinely ordered to determine a person's general health status	Tracking of information about tests that are routinely ordered to determine a person's general health status

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?*

PII and PHI is reviewed for accuracy as it is collected and utilized to care for Veterans. Once the information is collected, it is entered into the national ID management system, which further verifies accuracy of Veteran PII. To ensure that collected information is correct and up to date, during the check-out process individuals are asked to confirm the accuracy of the information that was entered in the system and to update them with any new information. MHV does not produce any data or information.

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.

The MHV system does not create or make available new or previously unutilized information about an individual.

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 in Transit: All traffic is routed through the Trusted Internet Connection (TIC) gateway. Authentication proxies are managed by the VA TIC. MHV servers are within the VA accreditation boundary and within the VAEC-AWS cloud. Encryption is required for all external communications, i.e., FIPS 140-2 or current version. Data at Rest is stored in Amazon RDS, which supports encryption at rest for all databases using keys from the AWS Key Management Services. For the data at rest, the underlying storage is encrypted, which includes the automated backups, replicas, and snapshots. Encryption and decryption are handled transparently. The encryption for Amazon RDS uses the AES-256 standard encryption algorithm.

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).

Additional protections are in place such as Session Authenticity is provided using Transport Layer Security (TLS), PIV, or VPN access through advanced encryption standard (AES) with SHA1 authentication. VA-CSOC employs Intrusion Detection and Protection Systems (IDPS) used to monitor network traffic for malicious activity or policy violations.

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

PII/PHI is safeguarded using Oracle and AWS RDS databases which are required to be encrypted using a FIPS 140-2 compliant algorithm, as sensitive data resides in the MHV database.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

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

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

2.4a How is access to the PII determined?

MHV screening policies are consistent with applicable federal laws, executive orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position. All resources are screened for suitability before being given access to MHV systems and data.

All contractor appointments to MHV are subject to background investigations based on the risk level of the contractor's position.

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?

The minimum-security requirements for MHV's FISMA HIGH system cover VA security controls with regard to protecting the confidentiality, integrity, and availability for information processed, stored, and transmitted by MHV. The security-related areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; system and information integrity; and privacy. The MHV program employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in National Institute of Standards and Technology (NIST) Special Publication 800-53 and VA 6500 directives.

All controls are documented in the responding MHV AC SOP and the MHV Account Management Policy and the MHV Portals Account Management Policy which are all located on VA SharePoint and eMASS.

2.4c Does access require manager approval?

The MHV Contracting Officer's Representative (COR) ensures that authorized users of the VA information systems and the MHV Admin Portal are those who have an approved background screening. All system users (data custodians) are required to review and sign the VA Rules of Behavior (RoB) annually through the VA Talent Management System (TMS). Contractors must read and sign the RoB and complete security awareness and privacy training prior to receiving access to the information systems.

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

Yes, MHV retains audit records for the defined time period of at minimum one year, to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. All MHV logs are stored in the Security Information and Event Manager (SIEM) solution and are kept for a minimum of one year.

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

VA has appointed a VA Privacy Officer (PO) to the MHV project and mandated the PO responsibilities per the VA Handbook 6500 and VA Directive 6509. In addition, the VA Handbook 6500.2 (Management of Data Breaches involving Sensitive Personal Information) dictates the process for risk assessments, incident handling process, reporting, mitigation, etc. regarding breaches involving VA PII.

Section 3. Retention of Information

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

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

- Name (First, Last)
- Sex
- Social Security Number
- Date of Birth
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Current Medications
- Previous Medical Records
- Internal Control Number (ICN)
- MHV User ID

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

The SORN states that the PII data elements collected and maintained in records are disposed of in accordance with the records disposition authority approved by the archivist of the United States. Records from this system that are needed for audit purposed will be retained for at least six (6) years. Routine records will be disposed of when the agency determines they are no longer needed for administrative, legal, audit, research, or other operational purposes, but no less than 6 years. These retention and disposal statements are pursuant to the currently applicable NARA General Records Schedule GRS 3.2 Item 031.

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?

Records are maintained and disposed of in accordance with the records disposition authority approved by the Archivist of the United States. Records from this system that are needed for audit purposes will be disposed of 6 years after a user's account becomes inactive. Routine records will be disposed of when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes. These retention and disposal statements are pursuant to National Archives and Records Administration (NARA) General Records Schedules GRS 3.2, item 30 and GRS 3.2, item 31. Records are maintained and disposed of in accordance with the records from this system, 6 years. NARA guidelines as stated in RCS 10-1, records retention schedule, require retention for 75 years.

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

Records Control Schedule 10-1 link for VHA:
www.va.gov/vhapublications/rcs10/rcs10-1.pdf

Records Control Schedule VB-1, Part II Revised for VBA:
http://benefits.va.gov/WARMS/docs/regs/RCS_II.doc

National Archives and Records Administration: www.nara.gov

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.

MHV does not directly eliminate Sensitive Personal Information (SPI). The MHV system provides cloud hosting space for connected applications and their supporting databases; thus, the system does maintain the space used by the applications stated above to store PII and SPI. Refer to the Project Team security documentation for specific procedures for the elimination of SPI.

User access records and logs are maintained and disposed of in accordance with the records disposition authority approved by the Archivist of the United States. User access records and logs from this system that are needed for audit purposes will be disposed of 6 years after a user's account becomes inactive. Routine system access logs and records will be disposed of when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.

These retention and disposal statements are pursuant to NARA General Records Schedules GRS 3.2, item 30 and GRS 3.2, item 31. System access logs and records are maintained and disposed of in accordance with the Records from this system, 6 years. NARA guidelines as stated in RCS 10-1, records retention schedule, require retention for 75 years for Veteran PHR data. The data retention period has been approved by NARA and is processed according to the following:

- Records Control Schedule 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf

- Records Control Schedule VB-1, Part II Revised for VBA: http://benefits.va.gov/WARMS/docs/regs/RCS_II.doc

- National Archives and Records Administration: www.nara.gov

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the VA Directive 6500, VA Cybersecurity Program, NIST SP 800-88 rev 1, Guidelines for Media Sanitization and the VA Media Sanitization User's Guide (November 17, 2014).When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin.

Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction based on the VA Media Sanitization User's Guide. Additionally, facilities follow FSS Bulletin #209.1 National Media Sanitization and Destruction Program, as well as OIT-OIS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.
https://dvagov.sharepoint.com/sites/OITOIS/KnowledgeService/Pages/Information-Security-Policy.aspx

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.

MHV does not use real Veteran data in the Development and Test environments. Security controls following least privilege access and separation of duties are applied to the Production database. Procedures are in place to review log files after system modifications for potential PII or PHI. If these elements are found, defects are generated for system developers to modify code so that these elements will not be used or captured.

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 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: There is a risk that the information maintained by MHV could 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: To mitigate the risk posed by information retention, MHV adheres to the NARA General Records Schedule. MHV does not eliminate SPI; the data is kept indefinitely in accordance with the Records Control Schedule 10-1, approved by 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 MHV consists of 6 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by MHV 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
Corporate Data Warehouse (CDW) Data Mart	YES	YES	Medications	Part of Patient Medical Record	Information collected from CDW is pushed over secure Trusted Internet Connection (TIC)-compliant connections to MHV via secure / authenticated database to database connection.

National Portal-Liferay	YES	YES	• Name, First, Middle, Last • Sex • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone • Number, etc. of a different individual) • Medications • Medical Records • ICN, the VA Internal Control Number from the Master Person Index (MPI) • Previous Medical Records • MHV ID	To properly identify a Veteran	Only Veterans can access their information and access to the databases is limited based on need to know. MHV administrators do not have access to patient data. At VISNs, clinicians and support personnel are granted role-based access which is audited and managed by National Administrators.
Admin Portal- Liferay Admin	YES	YES	• Name, First, Middle, Last • Sex • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone • Number, etc. of a different individual) • Medications • Medical Records • ICN, the VA Internal Control Number from the • Master Person Index (MPI) • Previous Medical Records • MHV ID	To properly identify a Veteran	Only Veterans can access their information and access to the databases is limited based on need to know. MHV administrators do not have access to patient data. At VISNs, clinicians and support personnel are granted role-based access which is audited and managed by National Administrators.
National Portal-eVault	YES	YES	• Name, First, Middle, Last • Sex • Social Security Number • Date of Birth	To properly identify a Veteran	Only Veterans can access their information and access to the databases is limited based on need to know. MHV administrators do

			• Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone • Number, etc. of a different individual) • Medications • Medical Records • ICN, the VA Internal Control Number from the • Master Person Index (MPI) • Previous Medical Records • MHV ID		not have access to patient data. At VISNs, clinicians and support personnel are granted role-based access which is audited and managed by National Administrators.
HealthShare IRIS	YES	YES	All patient demographic updates sent from MPI to MHV.	To properly identify a Veteran	Access is limited to System Administrators; there are no accounts in IRIS
C32	YES	YES	• Name (First, Middle, Last) • Sex • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone • Number, etc. of a different individual) • Medications • Medical Records • ICN, the VA Internal Control Number from the • Master Person Index (MPI) • Previous Medical Records • MHV ID	To properly identify a Veteran	Only Veterans can access their information and access to the databases is limited based on need to know. MHV administrators do not have access to patient data. At VISNs, clinicians and support personnel are granted role-based access which is audited and managed by National Administrators.

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***
MHV API Service Consumer	APIs are used for both internal applications (e.g., National Portal, Admin Portal, Secure Messaging Clinician Portal) and external applications (e.g., VA.gov, VA Mobile) to transmit data securely across the network.	Can transfer any of the following depending on the API it is connecting to: • Name • Sex • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Medications • Medical Records • ICN (VA Internal Control Number from the Master Person Index (MPI)) • Previous Medical Records	Hypertext Transfer Protocol Secure **(HTTPS)**
Data Access Services (DAS) Single Point of Entry (SPOE)	The DAS SPOE is used to transfer data securely across the network between MHV and Oracle Health	• Prescription Number • Internal Entry Number (IEN) • Drug Name (Medication Name) • Provider • Placer Order Number	Hypertext Transfer Protocol Secure (HTTPS) and HL7

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***
		• Division Name • RESULT (MHV Refill Request Status) • DATE PROCESSED (MHV Refill Request • Status Date) • National Drug Code (NDC) • Dispense Date • Trade Name • Facility Phone Number • Drug schedule • VAMC Tracking Number • CMOP Tracking Number, CMOP Date Shipped, CMOP Carrier, Carrier Tracking • Number of RX in Package • Unique Index • LOGIN DATE (Last Refill Request Date) • DATE PROCESSED (Last Refill Process Date) • SENT_DATE • SENDER_TYPE • SENDER_ID • SENDER_NAME • Observation, Allergy Intolerance, Condition, • Goal, Immunization, Document Reference, • Diagnostic Report • ATTACHMENT_ID • USER_ID • Millennium Patient ID • Electronic Data Interchange Personal Identifier (EDIPI)	
Vets.gov API Service	The VA's "front door" for applications and login services	• Prescription Number • Internal Entry Number (IEN) • Drug Name (Medication Name) • Provider • Placer Order Number • Division Name • RESULT (MHV Refill Request Status) • DATE PROCESSED (MHV Refill Request Status Date) • National Drug Code (NDC)	Hypertext Transfer Protocol Secure (HTTPS)

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***
		• Dispense Date • Trade Name • Facility Phone Number • Drug schedule • VAMC Tracking Number • CMOP Tracking Number, CMOP Date Shipped, CMOP Carrier, Carrier Tracking Number • Number of RX in Package • Unique Index • LOGIN DATE (Last Refill Request Date) • DATE PROCESSED (Last Refill Process Date) • SENT_DATE • SENDER_TYPE • SENDER_IDSENDER_NAME • Observation, Allergy Intolerance, Condition, Goal, Immunization, Document Reference, Diagnostic Report • ATTACHMENT_ID • USER_ID	
Corporate Data Warehouse Data Mart (CDW)	Provides Veterans access to Medication List and Images. CDW is a central collection of standardized databases that integrate key VA clinical data to provide a complete view of the Veterans Health Administration (VHA) Record.	• Medication List • Images	**TCPS:** Data is pulled over secure Trusted Internet Connection (TIC)-compliant connections to MHV via secure/ authenticated database-to-database connection
Identify & Access Management / Master Person Index (IAM/MPI)	Provides authenticating Web service request; checks the system level authorization for invoking services	Searches, retrieves, and updates profile information. • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual)	Hypertext Transfer Protocol Secure **(HTTPS)**

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***
HDR - Pathways	Provides lab and allergy data that is loaded into the user's Personal Health Record (PHR) for the purpose of displaying within the web application and creating a PHR summary reports that can be taken to external provider appointments.	• ICN • Medical Record Info • Labs (Chemistry/Hematology) • Allergies	Hypertext Transfer Protocol Secure **(HTTPS)**
Patient Care Management Model (PCMM)	Used by MHV Secure Messaging to pull Primary Care Provider information to establish the correct triage groups for the patient inside the SM application.	• Medical Records • Name	JAX-RS interface over authenticated Hypertext Transfer Protocol Secure **(HTTPS)**
Personal Health Record (PHR)	Provides Veterans a copy of their Personal Health Record that includes VA medical information and self-entered data in a .TXT and .PDF format	• Medication • Medical Record	HTTPS/ Fast Healthcare Interoperability Resources (FHIR) Request
Single Sign-On Internal (SSOi)	IAM Shared Services - used by MHV to authenticate users against MHV systems, Personal Identification Verification (PIV) card or Active Directory (AD) to provide the ability to seamlessly authenticate between systems	• Name	Hypertext Transfer Protocol Secure **(HTTPS)**
Single Sign-On External (SSOe)	AM Shared Services - used by MHV to authenticate users against MHV systems, Personal Identification Verification (PIV) card or Active Directory (AD) to provide the ability to seamlessly authenticate between systems.	• Name	Hypertext Transfer Protocol Secure **(HTTPS)**
VA Profile	MHV will consume the VAPRO Profile API to retrieve Military Personnel Information. MHV will integrate with MPI as required to obtain the person of interest identity (active correlation).	• VAprofileID	Mutual TLS (mTLS) using x.509 CN

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***
VA Mobile Framework (VAMF) Mobile Appointments Services (MAS)	Used to pull more types of Appointments (Home Telehealth Appointments, Video Visits, and Appointments from the Cerner Millennium EHR system)	• Appointments	TCPS: TIC-compliant encrypted site-to-site VPN
VA Mobile Framework (VAMF) Patient Generated Data (PGHD)	Application that uses the VAMF platform to transmit patient-generated data from MHV to VAMF	• User First Name • User Middle Name • User Last Name • ICN • SSN • Email • Sex • Birth date • MHV ID / DFN • EDIPID	Hypertext Transfer Protocol Secure **(HTTPS)**
Veteran Benefits Handbook Interface (VBH)	Veteran Benefits Handbook Interface (VBH)	• MHV ID • User First Name • User Middle Name • User Last Name • ICN • Medical Record	Hypertext Transfer Protocol Secure **(HTTPS)**
Veteran Health Information Exchange (VHIE) – Direct Secure Messaging	Interface through which MHV allows its users who qualify to send MHV PHR information to participating community health partners via the VHIE interface	• ICN • Date/timestamp	SOAP web services over Hypertext Transfer Protocol Secure **(HTTPS)**
Veterans' Health Information Systems and Technology Architecture (VistA)	Interface through which MHV retrieves and updates a patient's EHR data stored in VistA to improve accessibility of the EHR sent to the patients when requested	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Medications • Medical Records • ICN (VA Internal Control Number from MPI) • Previous Medical Records • MHV ID	HL7 over Minimal Lower Layer Protocol (MLLP)

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***
VistA Imaging Service (VIX)	Enterprise service for retrieving patient centric imaging data from distributed VistA Imaging systems; in response to a user requesting their imaging data, MHV sends patient data through a web service interface	• Medications • Medical Records • ICN (VA Internal Control Number from MPI) • Previous Medical Records • MHV ID	Hypertext Transfer Protocol Secure **(HTTPS)**
VistA Interface Adapter (VIA)	Interface through which data is loaded into the user's PHR for the purpose of displaying the data within the MHV application and creating PHR summary reports that can be saved and taken to an external provider appointment	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Medications • Medical Records • ICN (VA Internal Control Number for MPI) • Previous Medical Records • MHV ID	SOAP and REST web services over Hypertext Transfer Protocol Secure (HTTPS)
IRIS / NewWay / RightNow	Help Desk contact application to which MHV transfers users after having established a session	• Session information • MHV identifiers (MHV ID)	REST web services over Hypertext Transfer Protocol Secure **(HTTPS)**
MHV SAML Identity Provider	Used by service providers (Mobile, VA.gov/ID.me) to allow their users who have MHV accounts to authenticate using their MHV credentials	• SAML Single Sign On (SSO) • SAML Single Logout (SLO) • Users' Authentication Credentials	Security Assertion Markup Language (**SAML**) Hypertext Transfer Protocol Secure **(HTTPS)**

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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: The privacy risk associated with maintaining PII is that the sharing of data within the VA could occur, and the data may be disclosed to individuals who do not require access, which increases the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to. Information collected is used only for authorized purposes per the Privacy Act as noted in the Privacy FAQ web portal. The MHV program provides a web-based application for Veterans, their families, and care providers to access health resources in an online environment. Certain information that is provided to the system is self-entered by the Veteran on a voluntary basis.

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***
ID.me	To allow ID.me users to consume MHV Identity Provider Services	• MHV User ID • Patient ICN • MHV Account Info, which is JavaScript Object Notation (JSON) data that includes account type and available service information	National Memorandum of Under-standing/ Inter-connection Security Agreement/ (MOU/ISA)	Hypertext Transfer Protocol Secure (HTTPS)

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 privacy risk associated with maintaining PII is that the sharing of data outside of the VA could increase the risk that data may be disclosed to individuals who do not require access, which increases the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by MHV personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within.

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 MHV Privacy Policy, as provided on the MHV web site, is attached in Appendix A.

The MHV System of Records Notice (SORN), listed as number 130VA10, can be located at the following URL:
https://www.govinfo.gov/content/pkg/FR-2024-02-23/pdf/2024-03715.pdf

6.1b If notice was not provided, explain why.

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

General Disclaimer: You must agree to these terms and conditions to use my HealtheVet. In the MHV Notice of Privacy (See MHV Privacy Policy in Appendix A), it states: “You do not have to provide the information requested for My HealtheVet registration, but if you choose not to provide it, we will be unable to process your request and deliver to you My HealtheVet online services. Your decision not to provide this information will have no effect on any other benefits to which you may be entitled.” This notification clearly explains the purpose for collecting information but offers the Veteran the option to not provide that information and informs them not providing it will have no effect on their health benefits. They simply will not be allowed to access all services offered through the My HealtheVet web portal application.

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 using MHV have the opportunity and right to decline to provide information. Failure to provide information may result in denial of access to MHV services.

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.

Individuals have the right to consent in accordance with the Privacy Act of 1974: “No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains [subject to 12 exceptions].” 5 U.S.C. § 552a(b). Individuals also have the right to consent in accordance with the HIPAA Privacy Rule, 45 CFR 164.502: The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain patient consent for uses and disclosures of protected health information for treatment, payment, and health care operations. An authorization is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule. Where the Privacy Rule requires patient authorization, voluntary consent is not enough to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: 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 members of the public may not know that the MHV system exists within the VA or that enough privacy notice has been provided.

Mitigation: The VA and MHV mitigate this risk by notifying the public that the MHV system exists, as discussed in detail in question 6.1: The System of Record Notice and in the Privacy Policy as provided on the MHV web site.

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 information in MHV is obtained electronically from other systems listed in section 1.2 of this PIA and individuals are not able to gain access to their information directly. MHV provides links within the portal to the VA Privacy Service which explains the provisions to permit the collection, use, maintenance and sharing of PII. The link is located with the following MHV page:
https://www.myhealth.va.gov/mhv-portal-web/web/myhealthevet/system-use-notification

Within the VA Privacy Service portal, links are provided to the most up-to-date VA Handbooks and Directives. VA Handbook 6300.4 (Procedures for Processing Requests for Records Subject to the Privacy Act) details the process in which individuals are notified that their PII information has been corrected or amended.

Individuals wishing to obtain more information about access, redress, and record correction of MHV data should contact the Director of Standards and Interoperability, Chief Health Informatics Office / Office of Informatics and Analytics / Veterans Health Information, Department of Veterans Affairs, 810 Vermont Avenue NW., Washington, DC 20420.

Department of Veterans Affairs (VA) Privacy Act Notice for "My HealtheVet (MHV)" (130VA10):
https://www.govinfo.gov/content/pkg/FR-2024-02-23/pdf/2024-03715.pdf

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)?

MHV is not exempt from the access 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?

MHV is a Privacy Act system.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The MHV SORN (130VA10/89 FR 13806) provides processes for individuals to have inaccurate PII corrected or amended (see the MHV SORN for specific addresses). "RECORD ACCESS PROCEDURE: Individuals seeking information regarding access to and/or contesting of records in this system may write or call their local VHA facility and/or the My HealtheVet Chief Information Officer." Furthermore, the VA Privacy Service provides a How To link to "Write a Privacy Act Request Letter "and to "Request a Record Amendment": https://www.oprm.va.gov/privacy/privacy_howTo.aspx

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.

MHV provides links within the portal to the VA Privacy Service which explains the provisions to permit the collection, use, maintenance and sharing of PII. The link is located with the following MHV page: https://www.myhealth.va.gov/mhv-portal-web/web/myhealthevet/system-use-notification. Within the VA Privacy Service portal, links are provided to the most up-to-date VA Handbooks and Directives. VA Handbook 6300.4 (Procedures for Processing Requests for Records Subject to the Privacy Act) details the process in which individuals are notified that their PII information has been corrected or amended.

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 MHV SORN (130VA10) provides processes for individuals to have inaccurate PII corrected or amended (see the MHV SORN for specific addresses). "RECORD ACCESS PROCEDURE: Individuals seeking information regarding access to and/or contesting of records in this system may write or call their local VHA facility and/or the My HealtheVet Chief Information Officer."

Furthermore, the VA Privacy Service provides a How To link to "Write a Privacy Act Request Letter "and to "Request a Record Amendment": https://www.oprm.va.gov/privacy/privacy_howTo.aspx

http://www.va.gov/foia/

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: There is a risk that individuals may improperly seek access to or redress regarding records about them held by the VA Office and become frustrated with the results of their attempt.

Mitigation: By publishing this PIA and the applicable SORN, VA makes the public aware of the unique status of applications and evidence files, such as those stored on the MHV platform. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

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?

MHV contractors are all subject to background investigations corresponding to the risk level of the contractor's position. VA requires a VA-specific background investigation or a formal reciprocation of the employee's current investigation. Because MHV stores and transmits Veteran health data, all new hires will need a Tier 4 high-risk public trust Background Investigation (BI) as required for access to systems containing PHI and/or PII. The MHV Account Management-Access Control Policy dictates specific criteria for access to the various administrative part of the Portal.VA employees are provided specific VISN access but must also comply with VA policies for Access Control as stated in the MHV Account Management and Portals Account Management Policies.

All individuals who use or gain access to VA information systems must read, understand, and agree by signature to adhere to the VA National Rules of Behavior (RoB) before they can be authorized to access VA information systems. Annual training for the VA National RoB is performed through the VA Talent Management System (TMS). At the end of the training session, users agree to comply with all terms and conditions of the National RoB by signing a certificate of completion. This training and agreement to abide by the Rules of Behavior must be renewed annually.

Veterans who wish to gain access to the portal must comply with NIST SP 800-63-2 LOA2 identity proofing requirements. For in-person identity proofing, Veteran users must provide two forms of ID that meet the requirements of the U.S. Citizenship and Immigration Services Form I-9. Accepted forms of ID include an unexpired U.S. passport and a current driver's license. For phone identity proofing, Veteran users can only use this method to verify identity if they received a VA direct deposit payment by Electronic Fund Transfer (EFT), like a disability compensation or pension payment. The Veteran must provide their full name, Social Security Number (SSN), checking or savings account number, and the dollar amount of their most recent EFT. For online identity proofing, Veteran users are verified using ID.me, a trusted partner that provides the strongest identity verification system available to prevent fraud and identity theft.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

No users from other agencies have access to the MHV system.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

<u>Admin Portal and SM Portal Roles</u>

Administrative Portal – The MHV Administrative Portal allows staff to Manage User Roles and perform In-Person Authentication. (IPA). Granting access to specific roles within the MHV Administrative Portal allows VA employees to administer the MHV application and control the implementation of additional features and functions. Once a Veteran is authenticated then they have full access to the MHV Application. It is critical that all employees who are granted access at any level to the MHV Administrative Portal have the appropriate level of training and understanding regarding the privacy and security of patient information.

National Administrators –The highest level of authority in the Manage User Role portlet. A person who has this role assigned is able to assign all other roles within the administrative portal. Because of the nature of Manage User Role functionality they must first assign a role to themselves in order to assign roles beneath that role.

ROI Administrator – Has no functionality associated with it at this time. It was originally able to manage holds on Personal Health Records for MHV users. The SSR requirement is being lifted through legislation very shortly and therefore there will be no need to have a hold on records pending this review.

Role Administrator – Persons with this role assigned have the ability to assign other staff as Authenticators. A person must complete the mandatory training for Role-Based Access in TMS prior to having this role assigned. Typically, this role is assigned to Chief, HIMS and MHV Coordinators. Role Administrators are also responsible for making sure that anyone they assign Authenticator rights to has the appropriate training.

Authenticator – Persons with this role assigned have the ability to authenticate a VA patient thus allowing them to have access to key portions of their Electronic Health Record. They are responsible for checking for a valid government ID, making sure the Veteran has signed the appropriate ROI form and previously making sure they had viewed the MHV video (this is no longer required. Once they had validated all prerequisites they were able to authenticate Veterans.)

HIMS Privacy Officer – Has no functionality associated with it at this time. It was originally designed to allow access to run FOIA reports from the MHV Administrative Portal. FOIA Reporting is no longer available in the MHV Administrative portal.

SM Administrator – Persons with this role assigned have the ability to utilize the SM Administrative Portal to create triage groups, assign staff members to a triage group and then associate groups of patients to those triage groups. They are responsible for ongoing maintenance of the application and granting access to new employees and healthcare team members. In the future they will be able to set up associations to allow for SM workload capture.

Calendar Administrator – Persons who are assigned this role are able to add local, VISN, and national events to the MHV Calendar thus making them viewable by MHV users.

Help Desk Administrator – Persons who are assigned this role are responsible for maintaining the users in the Help Desk role.

Help Desk Staff – Persons who are assigned this role are able to access the Help Desk portlet to assist users of the MHV application and provide support to users who contact the MHV Help Desk.

National Portal Accounts

Basic Account (Registered Veteran Accounts) - Anyone who registers on the MHV system and whose identity is not matched to the Master Person Index (MPI) system. (AAL Level 1)

Premium Account (Veteran Identity Proofed Accounts) - Anyone who registers on the MHV system using identity traits that is matched to the Master Person Index (MPI) system AND who has completed an Identity Proofing process (In Person or Remote) to use all features in MHV based on whether they are a VA patient or not. (AAL Level 2)

MHV Web Portal Administrators - MHV staff responsible for managing and maintaining the MHV system with various levels of access granted based on need to know.

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

Yes, contractors have access to the MHV system. The contractors who provide support to the system are required to complete and sign the annual Rules of Behavior Memo and complete the VA Privacy and Information Security Awareness and Rules of Behavior training via the VA's TMS.

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

All contractors are cleared using the VA background investigation process and must obtain a Tier 4 and Special Sensitive Rating (SSBI). Aside from the VA contractor requirements already specified in this section, MHV contractors are not specifically required to sign additional NDAs or confidentiality agreements. MHV contractors are required to comply with all VA policy regarding access to systems and PII and access is granted to each system based on a need to know/ least privilege concept.

8.2c. Does the contractor have a signed confidentiality agreement?

Yes, under the Business Associates Agreement between VA and By Light Professional IT, LLC.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

Yes, By Light has a BAA for all contractors and subcontractors.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
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.

No

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

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

VA ensures that all MHV personnel provide certificates of training annually for VA Privacy and Information Security Awareness training.

All members of the MHV project team are required to sign a Rules of Behavior (RoB) agreement prior to being given access to MHV systems. Additionally, the RoB is required to be reviewed and signed annually by each user. Annual training for the National RoB is performed through TMS.

There are two versions of the National RoB: one for VA employees and one for contractors. Following are the definitions of VA employee and VA Contractor:

- VA Employees - VA employees are all individuals who are employed under title 5 or title 38, United States Code, as well as individuals whom the Department considers employees such as volunteers, without compensation employees, and students and other trainees.

- VA Contractors - VA contractors are all non-VA users having access to VA information resources through a contract, agreement, or other legal arrangement. Contractors must meet the security levels defined by the contract, agreement, or arrangement. Contractors must read and sign the Rules of Behavior and complete security awareness and privacy training prior to receiving access to the information systems.

Users agree to comply with all terms and conditions of the National Rules of Behavior by signing a certificate of training at the end of the training session.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* ***Approved***
2. *The System Security Plan Status Date:* ***12/09/2024***
3. *The Authorization Status:* **Authorization to Operate (ATO)**
4. *The Authorization Date:* **03/25/2024**
5. *The Authorization Termination Date:* ***3/25/2025***
6. *The Risk Review Completion Date:* **12/05/2024**
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 No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related *to privacy control UL-1, Information Sharing with Third Parties.* ***(Refer to question 1.8 of the PTA)***

Cloud Technology Used: VAEC-AWS GovCloud High
Types of Cloud Models: IaaS and SaaS

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.*

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

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.

PHILLIP CAUTHERS

Digitally signed by PHILLIP CAUTHERS
Date: 2025.04.16 12:13:43 -07'00'

Privacy Officer, Phillip Cauthers

JOSEPH DECOTEAU

Digitally signed by JOSEPH DECOTEAU
Date: 2025.04.16 15:51:27 -04'00'

Information System Security Officer, Joseph W. Decoteau

SEAN GOOD

Digitally signed by SEAN GOOD
Date: 2025.04.16 13:30:19 -06'00'

Information System Owner, Sean Good

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

VHA Notice of Privacy Practices, Effective Date: 09/30/2022
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

The existing System of Records Notice (SORN), listed as number 130VA10. The SORN can be located at the following URL:
https://www.govinfo.gov/content/pkg/FR-2024-02-23/pdf/2024-03715.pdf

MHV Privacy Policy link (verbiage provided below):
https://www.myhealth.va.gov/mhv-portal-web/web/myhealthevet/privacy-security

Privacy Policy

You do not have to provide the information requested for My HealtheVet registration, but if you choose not to provide it, we will be unable to process your request and deliver to you My HealtheVet online services. Your decision not to provide this information will have no effect on any other benefits to which you may be entitled.

My HealtheVet recognizes the importance you place on privacy protection on the Internet. We make every effort to protect that privacy and to keep your personal information private and secure when using My HealtheVet. We will not disclose your personal information to third parties outside VA without your consent, except to facilitate the transaction, to act on your behalf at your request, or as authorized by law. Certain administrative information, such as your full name, date of birth, social security number, sex, email address, user type and zip code are collected to provide you access to My HealtheVet and is subject to the Privacy Act of 1974 (5 U.S.C. 552a, as amended). Only authorized persons in the conduct of official business may use your personal, administrative information contained in the My HealtheVet Administrative system of records. Any unauthorized disclosure or misuse of your personal administrative information may result in criminal and/or civil penalties. You may file a civil action in a Federal District Court against VA if you believe that VA violated the Privacy Act.

For website management, information is collected for statistical and management purposes. This government computer system uses software programs to create anonymous, summary statistics, which are used for such purposes as assessing what information and My HealtheVet services are the most and least useful to users. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under Federal law.

My HealtheVet is a Department of Veterans Affairs (VA) computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided for only authorized uses. VA computer systems are monitored for security purposes and unauthorized access. During monitoring, information may be examined, recorded, and copied.

The Use of Cookies

A Persistent Cookie is a line of text that is saved to a file on your hard drive and is called up the next time you visit that website. This permits the website to remember information about your previous visits and use of the website. My HealtheVet uses Cookies and Tracking Technologies in accordance with the VA Privacy Notice (http://www.va.gov/Privacy/).

Security of Information

At all times, security maintenance and administration is an essential element of web site operation. My HealtheVet employs several levels of security to protect the personal identifiable information of registered users. When you enter in your personal information, My HealtheVet establishes a secure connection with your browser so your information is 'encrypted' or scrambled for transmission and viewing while you access your information. In addition, these security measures comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.

Password Protection

Your identification and password are protected using a security protocol which provides a transmission level of encryption between your browser and My HealtheVet servers. The connection icon area on your browser will change to "HTTPS" instead of "HTTP" when this security feature is invoked. Your browser may also display a lock symbol on the task bar at the bottom of your screen to indicate this secure transmission is in place.

Personal Responsibility for Personal Information

You are responsible for protecting the personal health information you print out or download. It is important to protect your information the same way you would protect your credit card or bank information. Do not leave your printed information in a printer. Do not save your downloaded information to a public computer.

Registration

We encourage you to register for a My HealtheVet account to access many of the available features and tools. Registration is not required for use of certain features such as our Health Library.

Logging In

When you register for a My HealtheVet account, access to your personal pages will be password protected. You will have five (5) attempts to enter the correct password before you are locked out of the system. We strongly recommend that you protect your password, do not divulge it to anyone, and change it on a regular basis. My HealtheVet will never ask for your password in an unsolicited phone call or unsolicited e-mail.

Logging Out

You should always remember to log out when you are finished accessing your My HealtheVet account. This prevents someone else from accessing your personal information that is available when you are logged in. It is important to always log out when you leave, share, or use a public computer (i.e., a library or Internet café). If you forget to log out, the My HealtheVet system will automatically time-out your session after a period of non-activity.

Saving of Passwords by Browser

Many Internet browsers (such as Internet Explorer and Google Chrome) allow users to save User IDs and Passwords. When prompted by a browser to save your My HealtheVet User ID and Password, you should decline this option. Saving user IDs and passwords could potentially allow persons to gain access to your computer and access your personal information.

Surveys, Questionnaires and Polls

My HealtheVet may use surveys, questionnaires, and polls to facilitate feedback and input from our users. When you respond to surveys, questionnaires or polls related to our site, this information is collected as anonymous, aggregated information and is used for statistical purposes and/or to improve the site.

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)