Privacy Impact Assessment for the VA IT System called:

My VA Health (HealtheLife)

Office of Electronic Health Record Modernization (OEHRM)

Date PIA submitted for review:

10/1/2020

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rital.Grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Raymond Walters	Raymond.Walters@va.gov	906-774-3300 x.32025
Information System Owner	Michael Hartzell	Michael.Hartzell1@va.gov	803-406-0112
Person Completing this Document	Anh Tran	Anh.Tran1@va.gov	202-390-8339

Abstract

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

The Department of Veterans Affairs (VA) My VA Health application is a web-based patient portal that provides Veterans a view into their Electronic Health Record (EHR), refill prescription, and schedule appointments. It also allows Veterans and their healthcare providers to communicate securely and submit information about their health. With My VA Health, Veterans have the ability to 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 PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? 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.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*

- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

The Department of Veterans Affairs (VA) My VA Health application is a web-based patient portal that provides Veterans a view into their Electronic Health Record (EHR), refill prescription, and schedule appointments. It also allows Veterans and their healthcare providers to communicate securely and submit information about their health. With My VA Health, Veterans have the ability to take a more proactive approach to managing their health and utilizing VA health services and benefits. My VA Health (MyVAH) is HealtheLife, a commercial-off-the shelf (COTS) application developed by Cerner Corporation and implemented by the VA Office of Electronic Health Record Modernization (OEHRM). MyVAH is integrated in the VA.gov portal and the existing VA patient portal (MyHealtheVet), as part of Department initiative to modernize its healthcare technology.

VA has elected to use Department of Deference (DoD) Electronic Data Interchange Personal Identifier (EDIPI) as the primary identifier (or medical record number) for the Joint Electronic Health Record system, to which the My VA Health application connects.

The collection of information is defined by System of Record Notice (SORN) 130VA10P2 – My HealtheVet Administrative Record-VA, Federal Register 193 FR 59991, which is based upon the Privacy Act of 1974, 5 U.S.C. 552a(e).

Section 1. Characterization of the Information

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

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

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

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

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

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

VA has elected to use Department of Deference (DoD) Electronic Data Interchange Personal Identifier (EDIPI) as the primary identifier (or medical record number) for the Joint Electronic Health Record system, to which the My VA Health application connects. The VA patient Integration Control Number (ICN) may also exist as a historical and alternative identifier for certain patient records.

PII Mapping of Components

My VA Health consists of one key component. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by My VA Health and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
HealtheIntent (Federal Enclave)	Yes	Yes	Name, SSN, EDIPI, DoB, address, email, phone number	Clinical care, patient record request	Transport Layer Security (TLS)

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

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

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

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

My VA Health receives (or collects) information from two major sources, HealtheIntent and the Joint EHR system. HealtheIntent is a cloud-based software platform that aggregates health data across the continuum of care. The data comes from disparate systems, including the Joint EHR, then is transformed and standardized, creating a longitudinal patient record that enables decision support, quality measurement, and analytics for population health management. The Joint EHR system is the replacement of the legacy VA EHR system, Veterans Information Systems and Technology Architecture or VistA, which supports more than 9 million VA healthcare enrollees worldwide. My VA Health will be running in parallel with and as an integrated part of the existing patient portal, MyHealtheVet (MHV).

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

As having stated in answer 1.2, MyVAH processes data from HealtheIntent and the Joint EHR system, where information is collected directly from patients, providers, and various outside sources by the VA using several methods, such as paper forms (enrollment form for VA health care), interviews and assessments with the individual, secure web portals, virtual private network (VPN) connection, e-mail and facsimile.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose. This question is related to privacy control AP-2, Purpose Specification.

My VA Health is a web-based personal health record system that provides Veterans and eligible individuals with information and tools they can use to increase knowledge about their health conditions, refill prescription, schedule appointments, request their healthcare record, foster better communication with their care providers, and improve their own health.

Information processed by/passed through MyVAH is for the following purposes:

- Pharmacy fulfillment – refill prescriptions
- Scheduling appointment with care providers
- Patient's (user's) request of care record history
- Communication between patient/user with their care providers

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

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

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

MyVAH does not directly check information for accuracy. The information is trusted as it is passed through to MyVAH. As a patient portal application, individuals can verify if their information shown by the system is accurate and if not, they have the right to obtain access to their records and request correction when necessary. Reference Section 7 for additional information.

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

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

The collection of information is defined by SORN 130VA10P2, Federal Register 193 FR 59991, which is based upon the Privacy Act of 1974, 5 U.S.C. 552a(e).
https://www.govinfo.gov/content/pkg/FR-2016-08-24/pdf/2016-20217.pdf

The authority for maintenance of the system is Title 38, United States Code §501.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

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

Privacy Risk: My VA Health collects PII and PHI. If this information was 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 offer assistance to the affected parties so that they may find help they need to get through their crisis. My VA Health

employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These security measures include access control, awareness and training, audit and accountability, configuration management, identification and authentication, incident response, etc. The system is hosted in a Federal Enclave which employs high impact security control baseline in accordance with NIST SP 800-53 Rev4 and applicable 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 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.

Information are used as detailed below:

- **Name**- Veteran identification used for display, verification and reporting purposes;
- **Social Security Number (SSN)**- Veteran identity trait used for linking My VA Health to HealtheIntent and the Joint EHR;
- **Electronic Data Interchange Personal Identifier (EDIPI)**- Primary identifier used for correlation of information between My VA Health and HealtheIntent and the Joint EHR;
- **Patient Integration Control Number (ICN)** – VA unique identifier where one exists; used by the system only for correlation of information from various internal VA sources not exposed to the end user.
- **Date of Birth**- Veteran identity trait used for linking My VA Health to HealtheIntent and the Joint EHR;
- Mailing Address- Veteran identity trait used for linking My VA Health to HealtheIntent and the Joint EHR;
- Phone Number- May be provided by users as a means of contact (not required);
- Fax Number- May be provided by users as a means of contact (not required);
- Email Address- May be provided by users as a means of contact and may be used for system notifications (not required);
- Emergency Contact: May be provided by users as a means of contact in case of emergency (not required);
- Medical Records- Supports Veterans/users in obtaining their VA health information;
- Pharmacy/Medication Records- Supports Veterans/users to review/report on medications they currently taking or have taken in the past as well as provides a means for refilling prescription(s) and tracking refill(s) as they are being shipped;
- My VA Health User ID- Unique identifier for User within the application;

- Place and date of registration for My VA Health electronic record access- My VA Health stores the creation date of the account for administrative purposes only. Since My VA Health is a web-based application, the physical location or place of registration is not captured or stored;
- Delegate and grantee user IDs associated with My VA Heath users – Identifies users that can act on behalf of the user account owner;
- Level of access to My VA Heath electronic services- Users are assigned roles that determine the level of access that users are given on the site (used to restrict/expose access to different user types);
- Date and type of transaction – audits of actions performed by the end user of the system are logged in the account activity log and only accessible by the user and relevant VA staff to use for the purpose of troubleshooting and gathering non-identifiable statistics on the system;

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

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

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

MyVAH supports analysis tools and reports generated by HealtheIntent. The application does NOT conduct independent reviews or analyses of Veteran data and information stored in the cloud environment.

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

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

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

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

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

Privacy Risk: There is a risk the information in My VA Health can be accessed and used beyond minimum necessary required by VA internal system admin users to perform official duties. Criteria, procedures, controls, and responsibilities regarding PII access are well documented as part of the system Authority-to-Operate (ATO) process in accordance with NIST SP 800-53 Rev 4 and VA Handbook 6500 – Risk management framework for the VA information systems – Tier 3: VA information security program. The VA OEHRM, in collaboration with DoD Healthcare Management Systems Modernization Program Management Office (DHMSM PMO) and the Federal Electronic Health Record Modernization (FEHRM), is responsible for assuring safeguards of PHI/PII in the Federal Enclave (OEHRM Joint EHR System). Due to the sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

Mitigation: VA employs a variety of security measures to MyVAH, similar to those measures being implemented for the legacy patient portal, the MyHealtheVet system, to ensure that the information is not inappropriately disclosed or released. These 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. All security controls have been implemented 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 800-37 and applicable VA Directives. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation; consistent with VHA Directive 1605.2, Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information.

Section 3. Retention of Information

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

3.1 What information is retained?

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

The information listed below is retained by My VA Health:

- Name;
- SSN;
- EDIPI and/or ICN;
- Date of Birth;
- Mailing Address;
- Phone Number;
- Fax Number;
- Email Address;
- Emergency Contact Information;
- Account Numbers;
- Current Medications;
- Previous Medical Records.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

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 6 years after a user's account becomes inactive. Routine records will be disposed of when VHA determines they are no longer needed for administrative, legal, audit, or other operational purposes. The retention and disposal statements are pursuant to National Archives and Records Administration (NARA) General Records Schedule GRS 3.2 items 30 and 31. Records are maintained and disposed of after 7 years.

NARA guidelines as stated in VA Record Control Schedule (RCS) 10-1 requires retention for 75 years. The data retention period has been approved by NARA and is processed according to the following:

- Department of Veterans Affairs, Records Control Schedule 10-1 January 2019 https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf
- Department of Veterans Affairs, Office of Information & Technology Record Control Schedule 005-1 (August 3, 2009) https://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
This question is related to privacy control DM-2, Data Retention and Disposal.

My VA Health operates using two (2) NARA approved retention schedules:

- Department of Veterans Affairs, Records Control Schedule 10-1 January 2019 https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf
- Department of Veterans Affairs, Office of Information & Technology Record Control Schedule 005-1 (August 3, 2009) https://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?
This question is related to privacy control DM-2, Data Retention and Disposal

My VA Health does not directly eliminate Sensitive Personal Information (SPI). The system follows two (2) NARA approved retention schedules as having stated in answer 3.3.

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what

controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

Certain types of testing maybe conducted when there is need for functionality modification or addition prior to deployment. The usage of PII/PHI in those tests, if any, must comply with the Federal Regulations listed below. In addition, as part of health care operations, VHA may need to train staff on new/modified system functionality. If PII/PHI is used in training materials, applicable VA/VHA directives must be followed. PII can be used in researches approved by the VA Institutional Review Board (IRB).

The following Federal Regulations are applicable to minimize the risk:

- 38 USC 5702 -researcher(s) must submit a written request to the Record Management officer in charge, stating purpose and duration of using the records for;
- 38 USC 5701 applicable to names and addresses;
- 38 USC 7332, applicable to Drug Abuse, alcohol Abuse, HIV Infection, and Sickle Cell Anemia Records; HIPAA Privacy Rule; Privacy Act of 1974; and
- 38 CFR 1.488 applicable to Drug Abuse, Alcohol Abuse, HIV Infection, and Sickle Cell Anemia Records.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

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

Privacy Risk: There is a risk that the information used by My VA Health could be retained for longer than 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, My VA Health adheres to applicable National Archives Record Act (NARA) General Record Schedules (GRS), particularly VA Record Control Schedules (RCS) 10-1 and 5.1 as having provided in answer to question 3.2

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
OEHRM – Joint EHR-Millennium	Clinical care	PII/PHI (see the full list of data elements in Answer #2.1)	Transport Layer Security (TLS)

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
OEHRM – CareAware MultiMedia (CAMM)	Clinical care	Name, SSN, EDIPI, Clinical data (cardiology and radiology images)	TLS
OEHRM – P2Sentinel	Patient record access monitoring/compliance	Name, SSN, EDIPI, clinical care data	TLS
Office of Information & Technology (OI&T) – va.gov	Public internet – VA information	Public internet, no PII/PHI	Trusted Internet Connection (TIC) compliant site-to-site Virtual Private Network (VPN) connection
OI&T – VA Sign-up Service	User authorization	Person alias, messaging aliases, Federated Principal Alias (FPA)	TLS - Hypertext Transport Protocol Secure (HTTPS)
OEHRM – Single Sign On External (SSOe)	User authentication	PII (username) SSOe is used by My VA Health to authenticate users	TLS

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Privacy Risk: The privacy risk associated with maintaining PII is that sharing data within the VA could happen and the data maybe disclosed to individuals who do not require access and heighten the threat of information being misused (Violation of the "Need to Know" principle).

Mitigation: Security measures such as Access controls, Identification and Authentication, Auditing, Personnel Security have been implemented to ensure the "Need to Know" principle is strictly adhered to by VA personnel managing the My VA Health system.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

Note: This question is #7 in the Privacy Threshold Analysis.

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

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

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

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

Data Shared with External Organizations

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

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

In compliance with OMB Memoranda M-06-15 and M-06-16, security and privacy controls will be implemented for My VA Health as being documented in the VA Enterprise Mission Assurance Support Service (eMASS) system.

- System and information are categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization process PII is identified accordingly.

- The VA has disseminated policies which direct and guide the activities and processes performed by its administrations (VHA, VBA, National Cemetery Administration (NCA)), offices, facilities, and programs. The policies are periodically reviewed to ensure completeness and applicability.

- The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for Veteran PII/PHI while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.

Internal protection is managed by access controls such as user authentication (user IDs, passwords and PIV, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a

Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Privacy Risk: N/A

Mitigation: N/A

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.
This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

- The My VA Health Privacy Notice, as provided on the My VA Health website, is attached in Appendix A;
- The System of Records Notice (SORN) applicable to My VA Health (130VA10P2) can be located at the following URL:
  https://www.oprm.va.gov/docs/Current_SORN_List_8_25_20.pdf
  http://vaww.vhaco.va.gov/privacy/Update_SOR/130VA10P2_FR.pdf

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 have the opportunity and right to decline providing their information. Failure to provide information may result in denial of access to My VA Health.

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 also have the right to consent in accordance with 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 (PHI) for treatment, payment, and health care operations. An authorization is required by the Privacy Rule for uses and disclosures of PHI not otherwise allowed by the Rule. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of PHI 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.

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

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

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Privacy Risk: There is a risk that members of the public may not know that My VA Health exists within the VA or that a sufficient privacy notice has been provided.

Mitigation: The VA and My VA Health mitigates this risk by notifying the public that My VA Health system/application does exist, as discussed in detail in question 6.1 (and Appendix A). The System of Records Notice link the Privacy Policy as provided on the My VA Health website.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

The electronic health records in My VA Health are collected electronically from other VHA systems listed in section 1.2 of this PIA. Individuals wishing to obtain more information about access, redress and record correction of My VA Health can contact the Director of Standards and Interoperability, Chief Health Informatics Office/Office of Informatics and Analytics/Veterans Health Administration, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington DC 20420 (Mailstop 130VA19).

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 electronic health records in MyVAH are collected electronically from other systems listed in section 1.2 of this PIA. Individuals wishing to obtain more information about access, redress and record correction of My VA Health can contact the Director of Standards and Interoperability, Chief Health Informatics Office/Office of Informatics and Analytics/Veterans Health Administration, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington DC 20420 (Mailstop 130VA19).

Patient/Veteran Right to Request Amendment of Health Information: You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.
If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal.
- File a "Statement of Disagreement".
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Reference VHA Handbook 1907.01 – Health Information Management and Health Records, section 26 – Health Record Alterations and Modification.
(https://www.va.gov/vhapublications/publications.cfm?pub=2&order=asc&orderby=pub_Number)

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.

Individuals wishing to obtain more information about access, redress and record correction of My VA Health can either contact the My VA Health Help Desk line 1-877-327-0022 or write to Director of Standards and Interoperability, Chief Health Informatics Office/Office of Informatics and Analytics/Veterans Health Administration, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington DC 20420 (Mailstop 130VA19).

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and

Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

The electronic health records in My VA Health are collected electronically from other systems listed in section 1.2 of this PIA. Reference the extraction of "Patient/Veteran Right to Request Amendment of Health Information" in Answer #7.2 above.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Privacy Risk: There is a risk that individuals may seek to access or redress records about them held by VA and become frustrated with the fruitless result of their attempt.

Mitigation: By publishing this PIA, and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored in the My VA Health system. Furthermore, this document and the My VA Health webpage provide contact information for members of the public.

Section 8. Technical Access and Security

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

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

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

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

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

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

My VA Health personnel screening policies are consistent with applicable U.S. federal laws, executive orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position. All VA human resources are screened for suitability before being given access to the system and data. All contractor appointments to the system are subject to background investigation using the Background Investigation Request Worksheet (BIRW), depending on the risk level of the contractor's position.

All VA personnel before being granted access to My VA Health must complete both the Privacy and HIPAA Focused and Information Security training courses. Specified access is granted based on the employee/contractor functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information Security Officer (ISO), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information. Users submit access requests based on need to know and job duties. Supervisor, ISSO and OIT approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes.

End user (Veteran and eligible individual) accounts are created when the Veterans register themselves. End user accounts (registered and in-person accounts) reside in Active Directory (AD).

VA employees can log in against AD and do not register on the admin portal. My VA Health system administrators are VA employees and therefore are not required to register through the My VA Health end user account registration workflow. VA employees log in to the admin portal using their AD account to perform admin functions. They can also be My VA Health end users and can log in with a My VA Health account using the account log-in link via Lightweight Directory Access Protocol (LDAP).

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

Yes, contractors can access My VA Health. Contracts are reviewed annually at a minimum. The contractors who provide support to the system are required to complete both the Privacy and HIPAA Focused training and Information Security training courses annually. All contractors must be cleared by means of the VA background investigation process and must obtain a Moderate Background Investigation (MBI) or full BI before their access right to PII/PHI can be granted. Aside from the VA contractor requirements already specified in this section, My VA Health contractors are not specifically required to sign additional Non-Disclosure Agreement (NDA) or confidentiality agreements. My VA Health contractors are required to comply with all applicable VA policies regarding access to systems and PII.

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

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

Personnel that will be accessing VA information or information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Security Awareness training which all personnel must complete via the VA Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. 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. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually.

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

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

MyVAH (HealtheLife) was structured as part of the Military Health System (MHS) Genesis ATO package, which was authorized to operate as High Impact system by the Defense Health Agency Authorizing Officer (AO) on May 18, 2020 for a period of one calendar year. VA OEHRM leverages the enterprise approved ATO reciprocity Memorandum of Understanding (MOU), "Authority to Operate (ATO) Reciprocity", dated January 24, 2018 to maximize scarce cybersecurity resources for due diligence, instead of redundant and unnecessary testing and/or reauthorization of a DoD ATO system.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

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).

My VA Health Privacy Notice

The Veterans Health Administration (VHA) 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 secure when using My VA Health. We will not disclose your personal information to third parties outside VA Veterans Administration without your consent, except to facilitate the transaction, to act on your behalf at your request, or as authorized by law. Only authorized persons when conducting official job performance responsibilities may use your personal information contained in the My VA Health Privacy Act system of records. http://vaww.vhaco.va.gov/privacy/Update_SOR/130VA10P2_FR.pdf

Your Health Information

The My VA Health website is a patient portal that provides a view into your VA Electronic Health Record (EHR). It also allows you and your VHA providers to communicate securely and submit information about your health. The information available for you to view through the My VA Health patient portal is not a comprehensive view of all the data in your VA EHR. When you send information to your healthcare provider through the My VA Health patient portal, VHA clinical policies will determine if that information will be stored in your VA EHR where it will be accessible to members of your care team and staff. Information that becomes a part of your VA EHR remains in your EHR even if you stop using the My VA Health patient portal. In accordance with VHA clinical policies, only secured messages that become part of your VA EHR will be viewable in the electronic health record.

Messages sent through the My VA Health patient portal may not be limited to your VHA provider. Your physician or other professional health care providers may designate other VHA personnel to manage and respond to your messages. These may include nursing or other administrative staff who review messages and either respond or route the message to a provider for a response. You should consider this before using the My VA Health patient portal messaging feature to communicate sensitive matters. You may prefer to discuss such matters directly with your specific VHA provider to better preserve your privacy.

Sharing

When the self-service VA Veteran Delegation portal becomes available, you may assign a VA Online Health Delegate access to your My VAHealth information. The VA Online Health Delegate who you granted delegate access to will be able to view your health information, submit health updates and message your VA care team through the My VA Health patient portal just the same as if that person is you. However, their name will appear as your VA Online Health Delegate submitting the information on your behalf. If you grant VA Online Health Delegate access to another individual to use the My VA Health patient portal, you acknowledge and accept responsibility for your decision to provide them access to potentially sensitive information. You may revoke VA Online Health Delegate access to your account at any time using the self-service VA Veteran Delegation portal.

My VA Health patient portal allows you to securely send your VA Visit Summaries to a Direct Address. By sending your VA Visit Summary, you acknowledge and accept responsibility for the security of your data. You own and control the sharing of information contained in the VA Visit Summary; therefore, by sending the summary you are directing VHA to send your VA Visit Summary to someone at a direct messaging address. Be sure the Direct Address entered is correct. The party you are directing VHA to send your VA Visit Summary to might use weaker standards than VA uses to protect your information. Once your VA Visit Summary is sent to another party, it may no longer be protected by federal privacy protections and could be shared with someone else by the person or organization receiving it.

Authorized Uses

For website management, information is collected for statistical and management purposes. This secure government computer system uses software programs to create anonymous, summary statistics, which are used for such purposes as assessing what information and My VA Health 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 VA Health website is hosted on a Department of Veterans Affairs (VA) purchased 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 VA Health website uses Cookies and Tracking Technologies in accordance with the VA Privacy Notice (http://www.va.gov/Privacy/). These cookies do not contain any personal information.

IP Addresses (Server Log Information). An IP address is a number automatically assigned to your computer whenever you access the Internet. All computer identification on the Internet is conducted with IP addresses, which allow computers and servers to recognize and communicate with each other. The My VA Health website collects IP addresses in order to conduct system administration, report Aggregate Information (as defined below) to affiliates or partners, and to conduct web site analysis. The My VA Health website will also use IP addresses to identify any connecting devices and aid in the identification of users that do not comply with the Terms of Use agreement or threaten the My VA Health patient portal service, web site, users, clients or others.

Security of Information

At all times, security management and maintenance are an essential elements of web site operation. My VA Health employs several levels of security to protect the personally identifiable information of registered users. When you enter your personally identifiable information, My VA Health 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 VA Health servers.

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 download your information to a public computer. Please be aware that opening a PDF file may cause a copy of

that document to be placed on the hard drive of the computer in a Temporary file folder. Always check the computer temporary file folder and delete any copies you may find there.

Logging In

To access My VA Health, you will need to use a VA approved credential such as MHV premium credential, DS Logon Premium/level 2 or ID.me. Based on the login credentials you use you may be locked out of the system after multiple failed login attempts. If you are locked out of the system, you must wait before that credential can be used again. We strongly recommend that you protect your password, do not divulge it to anyone, and change it on a regular basis. VA is implementing more login security known as two-factor authentication. The VA approved credential you may select to use may require you to enter in a pin number or additional information other than a User ID and Password.

Please contact the Help Desk associated with the credential you select to use for assistance with registration and password resets.

Logging Out

You should always remember to log out of everything that you opened or viewed during your session when you are finished accessing your My VA Health account. This prevents someone else from accessing your personal information that is available when you are logged in. Always remember, it is important to always log out when you leave, share, or use a public computer (i.e., a library or Internet café). Remember that you will also need to log out of any access domains used such as MHV premium credential, ID.me or DS Logon. If you forget to log out, the My VA Health 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 remember your My VA Health 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 without your consent or knowledge.

Surveys, Questionnaires and Polls

My VA Health may use surveys, questionnaires and polls to facilitate feedback and input from you. 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. You may receive clipboard patient questionnaires from your healthcare team or select to update and submit your health information. These questionnaires will go be sent to your healthcare team as identifiable information and may be saved to your VA EHR.

Changes

This notice may be revised periodically. The most recent privacy notice will be posted on the My VA Health Patient portal. When significant changes are made that impact the collection and use of your personal information, a notification message will display in the patient portal upon your next login. We recommend that you read the policy whenever you visit the My VA Health patient portal.

Signature of Responsible Officials

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

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2020.10.13 18:26:31 -04'00'

PO, Rita Grewal

Raymond E. Walters 1578937

Digitally signed by Raymond E. Walters 1578937
Date: 2020.10.14 06:30:27 -05'00'

Information Security Systems Officer, Raymond Walters

Michael J. Hartzell 3487012

Digitally signed by Michael J. Hartzell 3487012
Date: 2020.10.13 16:47:00 -04'00'

System Owner, Michael Hartzell