Privacy Impact Assessment for the VA IT System called:

Whole Health Mobile (WHM)

Patient Centered Care and Cultural Transformation

Veterans Health Administration

Date PIA submitted for review:

26 August 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kimberly Murphy	Kimberly.Murphy@va.gov	781-331-3206
Information System Security Officer (ISSO)	James Mark McGee	James.mcGee5@va.gov	520-358-3247

	Name	E-mail	Phone Number
Information System Owner	Todd Houck	Todd.Houck@va.gov	412-310-2822
Data Business information Owner	Benjamin Kligler	Benjamin.kligler@va.gov	202-401-0308

Abstract

The Live Whole Health (LWH) mobile application enables all users to navigate the comprehensive array of currently available Veteran Administration (VA) tools, resources and capabilities that support Whole Health. Through the Whole Health approach, users have access to health Coaches, health and well-being information, education on managing their health and a host of resources that support the user's achievement of their personal health goals.

Overview

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

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

The Live Whole Health (LWH) mobile application is a coaching application to assist users to complete personal health inventory, determine goals and action steps, and pursue what matters most in their lives. There are native iOS and Android clients that support internal and external users. Mobile clients connect to a general support REST API that persists data from the mobile clients. The Live Whole Health mobile application enables all users to navigate the comprehensive array of currently available Veteran Administration (VA) tools, resources and capabilities that support the Whole Health approach. The LWH mobile application has two interfaces: the coaching app and the users app. The user's app allows enrolled Veterans to have access to health coaches, and all users to access health and well-being information, education on managing their health and a host of resources that support the user's achievement of their personal health goals. In addition, VA employees have access to Employee Whole Health activities. Coaching is where the coaches engage with enrolled Veterans to help them achieve their individual health goals by sharing information and inviting them to participate in Whole Health activities.

There is a cloud service provider with Amazon Web Service (AWS) via Octo, and the contract number is Prime Contract VA118-16-D-1015. This network will have a secure site-to-site connection with the VA. VA employees using the Live Whole Health Coaching application will only be able to access the application from within the VA Network.

The FedRAMP compliant data center/cloud environment owned and operated by AWS will use a variety of technologies to deliver continuous uptime and availability. LWH is housed in the High Availability Zone in – USGOV East Region, Northern Virginia.

The LWH mobile application is designed to empower users to improve their health and wellbeing.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>

- VHA Enrollment Status

PII Mapping of Components

Whole Health Mobile consists of (0) key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Whole Health Mobile and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A	N/A	N/A	N/A	N/A	N/A

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

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

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

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

The source of information is provided directly from the Veterans, VA employees, and the general public. It collects basic user file information.

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.

Users provide their information during the registration on the Live Whole Health mobile application. Collection of data is also collected from the ID Token (SECID, ICN, and MHV identifier).

ID Token user claims:

- "fediamMVIICN": "1008709788V230034"
- "fediamsecid": "0001739928"
- "fediamMHVIEN": "NOT_FOUND"

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

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

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

Enrolled Veterans are verified by local Whole Health staff (i.e., Coaches) by checking the profile information against the VA's medical record or VistA. Collection of data is also collected from the ID Token (SECID, ICN, and MHV identifier).

ID Token user claims:

- "fediamMVIICN": "1008709788V230034"
- "fediamsecid": "0001739928"
- "fediamMHVIEN": "NOT_FOUND"

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

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

The authority to collect this information is derived from SOR: U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, 9830, and 12107. VA 6500, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: Loss of Privacy Data - WHM handles PII information and there is a risk that the information may be improperly accessed or defaced. Collection of more information than is needed

Mitigation: To mitigate against this risk, least privilege and the use of FIPS 140-2 encryption modules. VA employees will have access to the system and must utilize a PIV to gain access. Veterans access the WHM application user interface using their username and password. Only system administrators have access to user PHI/PII information. All PII/PHI information are encrypted in the database. Only approved system admins have access to the database based on their role and least privilege. All PII/PHI information are encrypted in transit utilizing TLS 1.2.

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.

Internal to VA:

- Name – patient/clinician identification
- DOB – patient identification
- Personal email – patient communication

The PHI/PII information will be used by VA Whole Health Leads and Veterans in managing and improving their health. The information will help Coaches ensure content that is shared through the application is of interest to the user and supports their Whole Health goals.

External to VA:
No external connections exist to share data.

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

Third party tools are utilized to perform any data analysis for reporting such as Firebase, Crashlytics, and Google analytics tools are used. Analytics are gathered on the device and those are persisted in Firebase. The data is app usage not information about the user.

2.3 How is the information in the system secured?

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

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

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

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

Whole Health Mobile application is protected by VA Firewalls employed at the boundary of the system. The system is backed up daily (incremental) and weekly full backup. All data at rest in the database are encrypted. Data in transit are encrypted with TLS 1.2 or above to protect the confidentiality and integrity including PII/PHI information. All incoming and outgoing traffic (data in transit) from the web server is encrypted and transmitted through a VA Trusted Internet Connection (TIC).

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

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project? The information is only used to assist in helping the Veteran.

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.

WHM has employed least privilege. Only system administrators that have been approved with the assigned permissions have access to users PII/PHI information on the system. Privilege user activities and execution of privilege functions are all audited. All system activities are monitored and audited and sent to Splunk. Only system administrators have access to audit logs and are accessed as needed. Privilege user roles and responsibilities are reviewed regularly by the ISSO.

The information is only used to help the Employee and the Veteran with their health goals.

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?

VA employees and Veterans: Name, DOB, Personal email, Veteran's Status and VA Enrollment Status is the PHI/PII information retained in the system until the Employee retires, vacate the position, or when the Veteran leave the program.

Weight and Height are not directly requested. Users may share that information if they have a related goal, but it would be through a free-text entry at their discretion.

3.2 How long is information retained?

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

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

The information housed in WHM is related to VA personnel and Veterans for health advice. Information is retained for at least 5 years in alignment with guidance in the VA Handbook 6300.1 – Records Management Procedures and VA Directive 6300 – Records and Information Management. In addition, per the contract VA118-16-D-1008 36C10B20N10080040, section 5.2.1, "…Support five-year data retention requirements," section 5.6. WHM complies with VA RCS 10-1, Item Number 3075.10 (b) for record retention.

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. (Stopped at 3.3)

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.

This is a cloud-based system where data is not housed within the VA network/authorization boundary. WHM complies with VA RCS 10-1, Item Number 3075.10 (b) (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf) for record retention. The vendor complies with FedRAMP and NARA requirements for data retention as well. VA has a contract (VA118-16-D-1015) with the vendor (Octo & AWS) on specific language related with data retention and the vendor's responsibility to ensure VA data is not compromised.

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

No data (provider information) is retained but is updated by the provider to ensure that the information is kept current. WHM will purge all data stored on the database at the end of the retention period.

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

WHM PII is not used for research or training. The application does not contain data, for research or training.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by WHM could be retained for longer than is necessary to fulfill the Veteran/Employee's health. Records held longer than required are at greater risk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation: To mitigate the risk posed by information retention, WHM adheres with FedRAMP and NARA requirements for data retention. Information is retained for at least 5 years in alignment with guidance in the VA Handbook 6300.1 – Records Management Procedures and VA Directive 6300 – Records and Information Management. VA has a contract (VA118-16-D-1015) with the vendor (Octo & AWS) on specific language related with data retention and the vendor's responsibility to ensure VA data is not compromised. WHM complies with VA RCS 10-1, Item Number 3075.10 (b) for record retention. WHM project staff will periodically review data retention thresholds such as the 5-year requirement and discuss options with VA before purging data.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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 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 Us

Data Shared with Internal Organizations

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

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:
Privacy Risk: Information is not being shared with any external organizations or in the VAEC. The data is application usage, not information obtained from the user.

Mitigation: The data is application usage, not information obtained from the user.

The Whole Health Mobile takes a defense-in-depth approach to protecting Employee and Veterans PII data to include the following protection mechanisms:
1. The Application's loader API protected by a policy enforcement/policy decision point
2. VA hosts in MAG are protect by FedRAMP High boundary protections at the hosting facility and only administrators have access to the administrative functions of the cloud services.
3. Data -at-rest encryption for any partition where PII will be contained
4. Data -in-transit encryption using TLS 1.2 on any network traffic beyond the local enclave.

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? There is no information or data shared or received internal or external.

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

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

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

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

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?
Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

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

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

To protect Veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:
1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.

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

4. Internal protection is managed by access controls such as user IDs and passwords, two-factor authentication, in addition: awareness and training, encryption, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:
Privacy Risk: WHM does not share information with external organizations in the VA. Analytics are gathered on the device and those are persisted in Firebase. The data is app usage not information about the user.

Mitigation: WHM does not share information with external organizations.

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.

WHM provides notice of information via the Privacy Act statement on applications completed by the Veterans on the app. At the time of entry, they are notified that the information may be transmitted to departments internal to the VA for regulatory and investigative purposes.

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

Whole Health Mobile receives its data collection from VA Partner Systems (VHA). VA Partner Systems (VHA) provide adequate notification by giving public notice of data collection via the Federal Register the Site Assistance component requests voluntary (optional) contact information if the requesting user wishes to have the support team contact them about their technical support issue. The veterans IP address is registered for security audit purposes only.

Veterans and employees may decline to enter information in the Application. Use of the Application is not a requirement. It is an available tool to assist with improving the health and well-being of the Employee and Veteran.

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

By agreeing to participate in Coaching with a VA Whole Health Lead, the individual consent to share their profile, PHI, and other information through the app with a VA staff Coaching member. VA staff will use the information to identify relevant material to assist the user on their Whole Health journey, invite the user to events, and wellness activities/challenges, and send messages/emails to the user.

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

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

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

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

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

Follow the format below:
Privacy Risk: Insufficient notice of information being shared may put an individual in a situation not prepared for and breach their privacy rights and trust. Information collected is from secured information systems with appropriate security controls in place. Individuals consent to their information being utilized for the purpose of advising on health-related issues.

Mitigation: Information collected in the WHM system is not disseminated/shared, and therefore it cannot risk insufficient notice.

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 employee can access their information through the VA authoritative data sources and the WHM Application. The PII/PHI collector follows the guidance of Office of Management and Budget (OMB) Circular A-130 when processing Privacy Act/FOIA requests from individuals. Procedures for adhering to a FOIA request are outlined in VA Handbook 6300.4: Procedures for Processing Requests for Records Subject to the Privacy Act**.**

In accordance with VA Directive 6300 and Handbooks 6300.3, Procedures for Implementing the FOIA, 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act, and VHA Directive 1605.1, Privacy and Release of Information an individual's submitting information requests may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned system of records, Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Veterans and employees input their personal information into the WHM application and can correct inaccurate information on their own.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans and employees input their own information in WHM. If information is incorrect, the Veteran/employee can correct the information when they log-in to the Application.

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.

Whole Health Mobile is a Coaching app, it is not the VA authoritative source for HR; however, it will receive employee information from VA's authoritative data source, through the VA SSO implementation to authenticate the users. If information is incorrect, the Veteran/employee can make corrections when they log-in to the application.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:
Privacy Risk: Data is managed by the user via the apps. Information is not pulled or pushing data to any VA or any other systems.

Mitigation: Data is managed by the user via the apps. Information is not pulled or pushing data to any Technology or any other system. Data is managed by the user via the apps. Information is not pulled or pushing data to any VA or any other systems.

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.

WHM has employed least privilege. Only system administrators that have been approved with the assigned permissions have access to users PII/PHI information on the system. Privilege user activities and execution of privilege functions are all audited. All system activities are monitored and audited and sent to Splunk. Only system administrators have access to audit logs and are access as needed. Privilege user roles and responsibilities are reviewed regularly.

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

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

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

Yes. VA Contractors (Octo group) developed and maintains the system. Contracts are reviewed annually at a minimum. Contractors who provide support to the system are required to complete an annual VA Privacy and Information Security Awareness and Rules of Behavior training via the VA's TMS. All contractors are cleared using the VA background investigation process and must obtain a Moderate Background Investigation (MBI) or full BI if they will be accessing PII or PHI. Aside from the VA contractor requirements already specified in this section, contractors are not specifically required to sign additional NDAs or confidentiality agreements. Contractors are required to comply with all VA policy regarding access to systems and PII. Per the contract (VA118-16-D-1015), contractors will complete annual TMS training requirements and submit certificates of completion to the COR to ensure proper training and awareness are enforced to act as deterrent to unauthorized disclosure of personnel data.

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.

There is no specific training for the VA APP or Coaching App. The App is readily available from either the Apple or Android store. VA Employees, and contractors are required to take the Annual VA Privacy and Information Security Awareness Training and Rules of Behavior through the Talent Management System (TMS). and supply certificates to their supervisor. Contractors must supply their certificate of completion to their COR.
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.

Veterans sign in through the website and are not required to train or sign Rules of Behavior or security awareness and privacy training.

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

If Yes, provide: No, this is a new system.

1. *The Security Plan Status*
2. *The Security Plan Status Date*
3. *The Authorization Status*
4. *The Authorization Date*
5. *The Authorization Termination Date*
6. *The Risk Review Completion Date*
7. *The FIPS 199 classification of the system (LOW/MODERATE/LOW*

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:***

Initial Operating capability date is approximately in March 2023 (ATO)

Section 9 – Technology Usage

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

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

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

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

Whole Health Mobile does utilize Cloud technology based on the VAEC platform. There is a FedRAMP ATO for VAEC. The full authorization package is available in OMB Max.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).
This question is related to privacy control UL-1, Information Sharing with Third Parties.

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).
This question is related to privacy control UL-1, Information Sharing with Third Parties.

The model used is Software as a Service (SaaS).

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

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

Yes. The contract number is V118-16-D-1015 Whole Health Mobile does not have access to this contract at the Project level.

9.4 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.

There is no ancillary data collected outside of the PII listed in section 1.1.

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

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

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

Yes. Specific language on data ownership and details around data management is detailed in the contract V118-16-D-1015

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

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

N/A - RPA is not utilized within the WHM product boundary.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties
WHM	Whole Health Mobile

Signature of Responsible Officials

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

Digitally signed by Kimberly E. Murphy 183320
Date: 2022.09.07 15:45:23 -04'00'

Privacy Officer, Kimberly Murphy

James M. McGee 926698

Digitally signed by James M. McGee 926698
Date: 2022.09.07 13:15:24 -07'00'

Information Security Systems Officer, James Mark McGee

TODD HOUCK

Digitally signed by TODD HOUCK
Date: 2022.09.13 12:46:31 -04'00'

System Owner, Todd Houck

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).