Privacy Impact Assessment for the VA IT System called:

HealthMain

Office of Community Care
Veterans Health Administration

Date PIA submitted for review:

09/26/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Penny Lashua	Penny.Lashua@va.gov	857-364-5938
Information System Security Officer (ISSO)	Andrew Vilailack	Andrew.Vilailack@va.gov	813-970-7568
Information System Owner	Harris Khan	Harris.Khan2@va.gov	703-789-7883

Abstract

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

HealthMain (www.healthmain.com), developed by Millennium Prevention, Inc., is a web-based platform that sets in one place a wealth of evidence-based tools and information resources to guide health promotion and disease risk reduction at individual and population levels, including:
•A 20-minute fully validated, self-administered health risk appraisal tool focusing on the main lifestyle factors linked to disease risk and designed to guide in-person and telephonic lifestyle counseling
•Optional validated self-administrated health risk appraisal tools to further guide in-person and telephonic behavioral lifestyle counseling
•A two-page Personalized Lifestyle Profile® that summarizes more than 30 health characteristics and dimensions of an individual's lifestyle behavior benchmarked against current expert clinical and behavioral health guidelines to target interventions
•Strategies for effective lifestyle behavior change designed to meet an individual's clinical needs and personal goals and preferences
•A personalized Lifestyle GPS® that defines the individual's baseline needs, such as age- and gender- specific calorie and nutrient requirements, and maps intervention progress over time toward goal achievement
•Systems, tools and analytics to monitor milestone achievement and reward success
•Communication tools to foster improved dialogue and client-centered care between individuals and their health care advisors
•The best available print and electronic health and prevention resources

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 IT system, HealthMain®, resides in the VA Enterprise Government Cloud is accessed at www.healthmain.com. HealthMain® is owned entirely and licensed for use by Millennium Prevention (MP), Inc, an innovative, research driven life sciences company and small women-owned business with a public health mission. Millennium offers health promotion and disease prevention resources on a comprehensive, secure, HIPAA-complaint, National Committee on Quality Assurance(NCQA)-certified web-based platform under the HealthMain® trademark. HealthMain® provides the first, fully- integrated, lifestyle-focused web framework to support healthcare professionals in behavioral counseling designed to treat and improve the management of preventable health problems including: overweight and obesity, hypertension, heart disease, diabetes and lifestyle-related cancers.

HealthMain® will be used to support healthcare professionals in the VA Boston Healthcare System (VABHS) who deliver prevention-focused services and programs, particularly those for weight management and related chronicdisease risks reduction within the existing VABHS MOVE! program. MOVE! is a national Veterans Health Administration (HVA) Directive aimed at addressing high rates of overweight and obesity and related chronic disease risk among adult male and female veterans. Current national research suggests that VHA MOVE! program participation and retention and intervention compliance rates are lower than optimal and health outcomes (rates of overweight and obesity and metabolic risk profiles) could be improved. The proposed VABHS-HealthMain® (HM®) innovation/quality improvement pilot offers a solution. MP's proprietary HM® technologies provide powerful, research-driven software platform frameworks that facilitate advanced, in-person and telephonic nutrition and lifestyle counseling that can be *personalized* to address the individual's unique biological needs, goals, and personal preferences. The flexible service delivery strategies offered by telephonic counseling and the targeted, personalized services, all facilitated by HM®, are designed to increase client access to preventative clinical services, program retention rates, and intervention compliance and improve outcomes.
These targeted services, made easy by HealthMain®, are designed to promote health and enhance the management and prevention of chronic diseases and improve service quality. To achieve client-centered care and manage personalized services, HM® incorporates current expert clinical practice guidelines (CPGs), the 2015-2020Dietary Guidelines for Americans (DGAs), and the U.S. Physical Activity Guidelines (PAGs) to guide targeted interventions and benchmark patient progress towards goal achievement. In addition, HM® software platforms offer a HIPAA-complaint and NCQA-certified environment suited to client-centered care and electronic health record integration, if desired.

Within MOVE! HealthMain® will be used to standardize the methods of delivering *personalized* weight management and related health risk reduction services, implement these service innovations, and assess theirimpact on service delivery quality improvement and veteran patient health outcomes. In so doing, we will

establish a 'proof of concept' (POC) model in the current VABHS MOVE! weight management serviceenvironment. Information gained from the proposed pilot will provide a foundation for future grant development and could serve as a model for the VHA nationwide.

The proposed VA-HealthMain® innovation/demonstration pilot will involve 120 male and female veterans who receive MOVE! services at one of three VABHS hospitals and related community health centers.

The proposed pilot is not a regional GSS, VistA, or LAN.

The HealthMain® web platform is organized into four major sections. The About You section contains the proprietary, validated and NCQA-certified health risk appraisal tools. VA patients will access the HM® platform viaa secure web link and provide self-reported demographic information, personal and family health history, selected clinical parameters (height, weight and waist circumference), and diet, physical activity and other
health-related lifestyle behavioral information. This self-reported information is benchmarked, using MP's proprietary algorithms, in comparison with current expert clinical practice guidelines to create a unique two - page report (Personalized Lifestyle Profile®) (PLP®) that identifies areas where the patient currently meets current health guidelines and other areas that can be targeted for personalized health improvement using evidence-based strategies. The PLP® is expanded into a 30-page report that explains strategies for modifying lifestyle behavior with research-driven methods known to improve health and reduce disease risk (a Lifestyle GPS®). Strategies are targeted, using HealthMain® technology, to each patient's unique biological needs, goals and personal preferences. Resources to support effective lifestyle behavior change are provided in three other informational sections of the HealthMain® platform (web-based sections called 'Nutrition', 'Health' and 'Living'). All resources are high quality and evidence-based and vetted by MP's professional team and updates as resources become available.

HealthMain® is a secure platform. Patient information is not shared without patient permission and consistent with HIPAA guidelines and Terms of Use. To facilitate client-centered care, patients can convert HM® reports to PDF format using the platforms tools and send them to their provider via HealthMain®'s electronic email link. In a HIPAA-complaint environment, PDFs are also suitable for viewing by the healthcare professional and elementscould be integrated into a patient's electronic health record, as appropriate to HIPAA and VA policies, the legal authority governing this project. and consistent with MP's Terms of Use and Privacy Protection policies (published at: www.healthmain.com.

HealthMain®, is only accessed via password-protected log-in on one secure site: www.healthmain.com.

Millennium Prevention, Inc. will grant the VABHS a license to use the HealthMain® platform in the proposed innovation/demonstration pilot initiative.

We don't anticipate this project will require changes in VABHS business processes. VABHS personnel will be trained to use the HealthMain® web platforms as a powerful resource for the improved delivery of their MOVE! weight management and related disease risk reduction services. Currently, VABHS provides these clinical services in scheduled in-person (individual and group) behavioral counseling services. HealthMain® will innovate and enhance service delivery with advanced technology that supports in-person and telephonic counseling.
Telephonic counseling currently is only provided on a limited basis and will be expanded in this polit project. Asa result, HM® will provide greater veteran access to MOVE! weight management. The personalized services facilitated by HM® will enhance client-centered care patient as advocated in all current expert clinical practice guidelines. Given that services can be provided telephonically, they can also be scheduled at greater convenience to providers and patients and improve client retention and compliance with intervention recommendations.
We don't anticipate technology changes in this pilot project; HealthMain® is a fully developed, HIPAA-compliant, NCQA-certified web platform with research-driven tools and resources and proprietary, tested functionalities and algorithms.

The Privacy Act system of records notice (SORN) that covers the information with the HealthMain® is

24VA10A7 Patient Medical Records – VA.

The HealthMain system does use cloud technology and does not yet have Federal Risk and Authorization Management Program (FedRAMP) provisional or agency authorization. The system is NCQA-certified and designed to be HIPAA-compliant.

Given that HM collects III, SPSI, IIHI and PHI on a cloud-based platform, there is some minimal risk to the individual were the system to become subject to an unauthorized data breach. Millennium Prevention, Inc. will maintain an MOU or Business Associates Agreement with VABHS consistent with the following regulations*:*

- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub L. No. 104-191 (Aug 21, 1996,codified in scattered sections of title 42 USC (full text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).

- Health Information and Technology for Economic and Clinical Health (HITECH) Act, Title XIII of division Aand Title IV of Division B of the American Recovery and Reinvestment Act of 2009, P.L. No. 111-5, 123 Stat. 226 (Feb 17, 2009) codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.

See our cloud-based security system's (Armor's) certifications: https://www.armor.com/certifications/ includingHITRUST.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Demographic information: name, date of birth/age, gender, race

Family and personal health history: chronic disease diagnosis: heart disease, diabetes, etc. Clinical measurements: height, weight and waist circumference; waist and health perceptionsDietary behavior: frequency of food intake and related dietary behavior assessment
Physical activity, tobacco use, alcohol intakePersonal health priorities
Additional general health information and lifestyle behaviors (helmet and seat belt use, hearing and visual acuity, etc. as required for NCQA certification)

PII Mapping of Components

HealthMain® consists of 0 key components.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

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					

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 HealthMain® web platform gathers self-reported information directly from the individual patient using secure on-line, cloud-based survey tools.

No data are imported from other sources.

With the clinical environment, clinicians may also collect measured clinical data, such as patient's weight and height, and advise patients to use this information in making their on-line survey responses. This improves system accuracy and improves validity of follow-up information on health outcomes.

HealthMain® also uses powerful proprietary algorithms to interpret the individual's responses and prepare reports to assess clinical and lifestyle-related behavioral risk (such as level of overweight or obesity, dietary nutrient quality, or physical activity level in relation to expert clinical guideline recommendations, etc.) and guide preventive interventions for personalized weight management and disease risk reduction targeted to the unique biological needs, personal preference and goals of the individual.

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.

HealthMain® is cloud-based. Patients use a password-protected, personal log-in to access on-line survey tools, including the core health risk surveys and resulting personalized reports. All are provided in HealthMain®'s HIPAA-complaint, FEDRAMP certified VA Enterprise Amazon Web Services Government Cloud environment.

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.

HealthMain® will be utilized in the VABHS MOVE! program to provide patient health risk appraisals and generate reports that support client-centered care and targeted, personalized counseling. While patients complete their on-line surveys, internal system tools are used to facilitate completion of each survey component. VABHS clinicians can also review patient on-line self-reported responses and advise patients where their responses canbe improved with measured clinical data (such as height and weight data and dietary and physical activity assessments) for improved accuracy. This is all completed within the guidelines defined in the MOU and Business Associate agreement between VABHS and Millennium Prevention and consistent with HIPAA and HITECH guidelines.

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 data we are going gathering are self-reported by the individual VABHS patient consistent with HIPAA, HITECH38 USC 5701.

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub L. No. 104-191 (Aug 21, 1996, codified inscattered sections of title 42 USC (full text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).

Health Information and Technology for Economic and Clinical Health (HITECH) Act, Title XIII of division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, P.L. No. 111-5, 123 Stat. 226 (Feb 17, 2009) codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.

38 U.S. Code § 5701. Confidential nature of claims.

The Privacy Act system of records notice (SORN) that covers the information with the HealthMain® is 24VA10A7, Patient Medical Records-VA. 85 FR 52406.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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: HealthMain®'s online survey tools collect self-reported PHI (bulleted in Section 1.1 and 2.1 below) that directly relates to the mission of the VHA MOVE! program, notably for improved weight management and reduction inrelated chronic disease risk. HealthMain® uses validated survey tools and proprietary, tested algorithms to benchmark the individual's PHI against current clinical practice guidelines. The system also generates individualized reports that constitute a research-driven method to deliver personalized services using sound strategies for improved weight management and chronic disease risk reduction.
Given that HM® collects III, SPSI, IIHI and PHI on a cloud-based platform, there is some minimal risk to the individual were the system to become subject to an unauthorized data breach.

Mitigation: HealthMain® is a HIPAA-complaint, NCQA-certified web platform. Our privacy policies are published on-line at www.healthmain.com.

The HealthMain AWS GovCloud (US) environment is maintained by the Federal Government and gives government customers and business partners a secure cloud solution that is compliant with the FEDRAMP High baseline. The AWS GovCloud (US) is operated and maintained by employees who are U.S. citizens on U.S. soil. AWS GovCloud (US) is only accessible to U.S. entities and root account holders that pass a screening process. Server-side FIPS 140-2 encryption is used to protect sensitive unclassified data files in the Amazon S3 environment. Access to sensitive data can be limited by individual, time and location and restrict which API calls users are allowed to make the platforms access control testing tools.

Millennium Prevention, Inc. will maintain an MOU or Business Associates Agreement with VABHS consistent withthe following regulations:

> Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub L. No. 104-191 (Aug 21,1996, codified in scattered sections of title 42 USC (full text); 45 C.F.R. parts 160 and 164 (HIPAAPrivacy and Security Rules).

> Health Information and Technology for Economic and Clinical Health (HITECH) Act, Title XIII of division Aand Title IV of Division B of the American Recovery and Reinvestment Act of 2009, P.L. No. 111-5, 123 Stat. 226 (Feb 17, 2009) codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.

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.

HealthMain® data will only be used internally for the purpose of the proposed innovation/quality improvement pilot. As an innovation and quality improvement initiative, we will be training existing MOVE! weight management professionals to use HealthMain® to enhance client-centered care through the delivery of personalized, lifestyle-focused services using both in-person and telephonic service strategies. Both strategies are in place currently but will be expanded and supported by HealthMain® platform innovations – including cloud-based tools, resources and analytics.

HealthMain collects the following PHI using on-line survey tools:

Demographic information: name, date of birth/age, gender, race
Family and personal health history: chronic disease diagnosis: heart disease, diabetes, etc.
Clinical information: height, weight and waist circumference, perceptions of health and weight status
Dietary behavior: frequency of food intake and related behaviors
Physical activity, tobacco use, alcohol intake
Personal health priorities
Additional general health information and lifestyle behaviors (helmet and seat belt use, hearing andvisual acuity, etc.)
Email
Date of Birth

Proprietary HealthMain® algorithms interpret self-reported PHI, interprets them by benchmarking the measurements and information against current clinical practice guidelines and produces a 2 page PersonalizedLifestyle Profile® with these results as well as a details 30-page report (a Lifestyle GPS®) which discussed research-driven strategies to promote better health in each of the lifestyle areas (diet, physical activity, etc.)u responses. These reports lay the foundation for enhanced client-centered care advocated in current expert clinical guidelines. These innovations facilitate personalized lifestyle counseling using both in-person and telephonic methods to reduce chronic disease risk and improve weight management. In addition, telephonic counseling, facilitated by HealthMain® will be scheduled at the convenience of the patient and provider and isanticipated to increase program referral, access and overall compliance and improve health outcomes – outcomes of interest in this innovation/quality improvement pilot.

Deidentified patient data sets will be used to complete the quality improvement and innovation assessmentsassociated with this project. We anticipate publishing our results in peer-reviewed publications.

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

HealthMain® proprietary algorithms benchmark the individual's self-reported demographic, clinical and lifestyle-behavioral data against current clinical practice guideline standards and reference points (for example, body mass index, an index of the individual's degree of overweight or obesity; estimated calorie requirements appropriate to the individual's age, gender, BMI, and level of physical activity). This information is utilized to guide the design of targeted strategies for improving diet, physical activity and other lifestyle characteristics and thereby improve weight management and reduce disease risk. Strategies such as these and which as supported by HealthMain® technologies are strongly advocated by current clinical practice guidelines.

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?

Secure Socket Layer (SSL)

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

The system does not collect, process or retain Social Security numbers.

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

All VA personnel including employees, contractors, volunteers, and students must be trained annually on privacy policies to include the requirements of Federal privacy and information laws, regulations, and VA policy. All VA personnel are responsible for compliance with VA's Information System Security policies. This training is required to be completed annually and access to VA information systems is not allowed

without it. All PII and PHI data are secured through the use of user identification and authentication (e.g., user id, password), and FIPS 140-2 certified endpoint encryption. This system uses FISMA standard processes for approving and monitoring access. This system is continually monitored and audited for compliance with FISMA security standards.

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

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

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

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

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

VA patients will access HealthMain® platforms after their Primary Care clinician's referral to this pilot. Patients who are referred to the MOVE! pilot will be asked to log into the secure HealthMain® platform where they create a password-protected account and accept Terms of Use and view Privacy Policy details. The patient uses their password to access the site, complete on-line health risk appraisal survey tools, generate and view reports, email their reports to their clinicians, provide platform feedback, and update their on-line profile to monitor milestone achievement and success during the pilot intervention.

VABHS Clinicians will be trained by Millennium Prevention under Dr. Halasz and Dr. Millen's guidance. They will use the HealthMain® to guide client-centered care and to facilitate patient use. Clinician access to HealthMain® is also password protected.

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

HealthMain® retains patient's on-line survey data information in the cloud-based environment of its server atArmor, Inc. (Richardson, TX). The pilot will be governed by the terms of the VABHS-Millennium MOU and/or Business Associate Agreement and consistent with HIPAA and HITECH policies.
The specific data retained include the following:
Demographic information: name, date of birth/age, gender, race, email, name and email of employees
Family and personal health history: chronic disease diagnosis: heart disease, diabetes, etc. Clinical information: height, weight, waist circumference, perceptions of health and weight statusDietary behavior: frequency of food intake and related behaviors
Physical activity, tobacco use, alcohol intakePersonal health priorities
Additional general health information and lifestyle behaviors (helmet and seat belt use, hearing and visual acuity,etc. as required for NCQA-certification)

In addition, HealthMain® algorithms interpret these data and create reports that benchmark the individual'sbaseline and follow-up guidelines against current clinical practice standards in order to guide the delivery ofprevention-focused services and measure program impact and service delivery improvement over time.

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 pilot and the data that it generates will be governed by the terms of the VABHS-Millennium MOU and/or Business Associate Agreement and consistent with HIPAA and HITECH policies as noted in 1.6. All data will be maintained consistent with VABHS retention control schedules as detailed in RCS 10-1 dated January 2019.

Department of Veterans Affairs (VA), Veterans Health Administration Record Control Schedule (RCS) 10-1,January 2019.

Temporary; destroy when business use ceases.

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

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

When managing and maintaining VA data and records, *HealthMain*® follows the guidelines established in the NARA-approved Department of Veterans Affairs (VA), Veterans Health Administration Record Control Schedule (RCS) 10-1 (March 2011) https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf,

Department of Veterans Affairs (VA), Office of Information & Technology RCS 005-1 (August 3,2009) http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf and the General Records Schedule (http://www.archives.gov/records-mgmt/grs/).

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

The pilot and the management of the data it generates will be governed by the terms of the VABHS-MillenniumMOU and/or Business Associate Agreement and consistent with HIPAA and HITECH policies.
All data will be maintained consistent with VABHS retention control schedules. Paper records are to be shreddedand electronic records are to be scrubbed when business use ceases.

The records may not be destroyed until VA obtains an approved records disposition authority from the Archivist of the United States.

Records will be destroyed according to NIST Special Publication 800-88.

Electronic media is sanitized based upon GovCloud Media Disposal Policy. Hard drives are overwritten using a multiple--pass write of complementary and random values to Department of Defense standards. The media is then destroyed by degaussing, shredding, or incineration).
During the interim, for the lifecyle of the data VA security protocols are followed throughout the system. The VAEC is a FISMA High environment and approved by VA to hold PII and PHI. This system is

protected by a myriad of security features including limited, approved access, encryption, network isolation, 24-hour security monitoring, auditing, security configuration, scanning, patching, personnel security as well as physical security required by FISMA and continually undergoes FISMA standard evaluations and reviews.

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

The pilot will be governed by the terms of the VABHS-Millennium MOU and/or Business Associate Agreement and consistent with HIPAA and HITECH policies.

HealthMain® uses on-line, validated survey tools to collect a limited set of self-reported demographic (name, age, gender) and clinical information (height and weight, and waist circumference, personal and family health history,perception of health and weight status) and lifestyle behavioral characteristics known to improve health and reduce disease risk (dietary behavior and nutrient intake, physical activity, smoking, alcohol use, etc.). The demographic, clinical and lifestyle behavioral data are collected in order to determine the appropriate clinical guidelines to use in benchmarking the individual's self-reported clinical and lifestyle behavior information against current expert guidelines for disease prevention and treatment including the US Dietary Guidelines and NIH Clinical Practice Guidelines for Obesity, Cardiovascular Diseases, and Diabetes prevention and treatment. Once the individual's self-reported data are benchmarked, a personalized report (absolutely unique to each individual)can be generated by the system to improve understanding of current clinical and lifestyle behaviors where guidelines are met and others that can be improved with targeted strategies (such as diet, weight loss, physical activity, etc.). This information supports personalized approaches to the design of prevention and chronic disease treatment strategies and; personalized client-centered clinical counseling is advocated in all current expert clinical practice guidelines. Personalized, client-centered care that is supported by the HealthMain® platform in a HIPAA-complaint, NCQA-certified environment and facilitates in-person and telephonic counseling adds key elements of innovation and quality improvement in the proposed pilot.

None of the PHI data gathered by the HM® on-line survey tools are disseminated beyond the clinicians involved in the pilot. Consistent with our MOU or Business Associate Agreement, deidentified PHI information could be aggregated if requested by VABHS to determine where MOVE! service delivery is being improved and where MOVE! program impact is being achieved as a result of this pilot.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: Given that HM collects III, SPSI, IIHI and PHI on a cloud-based platform, there is some minimal risk to theindividual were the system to become subject to an unauthorized data breach. The longer data are maintained, the higher the risk.

Mitigation: The pilot will be governed by the terms of the VABHS-Millennium MOU and/or Business Associate Agreement and consistent with HIPAA and HITECH policies:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub L. No. 104-191 (Aug 21 1996,codified in scattered sections of title 42 USC (full text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy andSecurity Rules).

- Health Information and Technology for Economic and Clinical Health (HITECH) Act, Title XIII of division Aand Title IV of Division B of the American Recovery and Reinvestment Act of 2009, P.L. No. 111-5, 123 Stat. 226 (Feb 17, 2009) codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

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			

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

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: There is a risk that information may be shared with unauthorized VA program or system or that data could be shared. The privacy risk is potential exposure of the limited data stored in this system. This system does not include the entire VA database but rather the partialdata of the subset of research subjects whose information would be currently being processed inthe system at the time.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access granted on a business need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access controlsand authorization are all measures that are utilized. This system is protected by a myriad of security features including limited, approved access, encryption, network isolation, 24-hour security monitoring, auditing, security configuration, scanning, patching, personnel security as well as physical security required by FISMA and continually undergoes FISMA standard evaluations and reviews. In addition, VABHS providers including WOC employees involved in this pilot, as appropriate, will be thoroughly trained on pilot project aims and scope, HealthMain® tools and resources and management including: Terms of Use and Privacy policies and all providers/employees will be subject to VA Handbook guidelines and maintain current human subjects training certification.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

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

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: Not Applicable. HealthMain® data is not shared outside of VABHS and this specific VA-HealthMain®innovation/quality improvement demonstration project.

Mitigation: Not Applicable. HealthMain® data is not shared outside of VABHS and this specific VA-HealthMain®innovation/quality improvement demonstration project.

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.

This pilot will be governed by the MOU and/or Business Associate Agreement between VABHS and Millennium Prevention, Inc and consistent with HIPAA and HITECH policies. VABHS clinicians will refer patients to the pilotand explain the scope of the pilot, consistent with VABHS clinical policies and our MOU/BAA.

The Privacy Act system of records notice (SORN) that covers the information with the HealthMain® is 24VA10A7, Patient Medical Records-VA. 85 FR 52406.

https://www.healthmain.com/privacy/

https://www.healthmain.com/terms/

https://www.healthmain.com/about/

https://www.healthmain.com/welcome/

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

All patients can elect, (i.e. opt in) to participate in the proposed VA-HealthMain® innovation/quality improvementprogram or not without penalty. Clinicians will make their patients aware of the opportunity and refer them to MOVE!, if interested. At any time prior to enrollment an individual can decline or drop out once enrolled.

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

Patients can decline participation in the pilot without penalty and drop their participation at any point, if desired. Patient compliance and provider adherence to protocols in routine clinical practice are critical to enhanced health outcomes and service quality improvement. We will strive to retain participants and believe the project innovations and ease of access afforded by in-person and telephonic counseling will lead to strong patient referrals, engagement, compliance, and continuation. We will also thoroughly train providers involved in this pilot to support successful outcomes.

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:

Given that HM collects III, SPSI, IIHI and PHI on a cloud-based platform, there is some minimal risk to the individual were the system to become subject to an unauthorized data breach.

Mitigation:

MP will enter an MOU or BAA for this project. VABHS and pilot participants will comply with to HealthMain®Terms of Use and Privacy policies**.** This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when veterans are enrolled for healthcare or research projects. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SOR) and Privacy Impact Assessment (PIA) available for review online.

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.

VHA Directive 1605.01 Privacy and Release Information', section 7(b) states the rights of the Veterans (or their proxy) to request access to review their records. VA Form 10-5345a, Individual's Request for aCopy of Their Own Health Information, 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 Records Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted. In addition, Individual patients have complete and open access to their HealthMain® information at all times, 24-7. They access the system by protected log-in.

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.

VABHS clinicians, trained on the use of HealthMain® by MP under Dr. Millen's supervision, can advise their patients on how to improve the accuracy of their information and update their on-line survey responses. In addition, all data entry to the individual patient is time-stamped and retained. Patients can log in andupdate or correct their data continuously throughout the pilot. This provides an on-line method for monitoring progress towards goal achieve, rewarding success, and measuring pilot outcomes.

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.

Patients update their own on-line data. All data entry and generated reports are time-stamped and trained for patient and provider use during the counseling process.

As in usual care and routine clinical practice, the individual patient's primary care provider or MOVE! counselor could advise on the need to correct information in the self-reported HealthMain® surveys.

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.

Patients update their own data in their password protected HealthMain® account. Their accounts are always available via the cloud.

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:
Given that HM collects III, SPSI, IIHI and PHI on a cloud-based platform, there is some minimal risk to theindividual were the system to become subject to an unauthorized data breach.

Mitigation:
The pilot will be governed by the terms of the VABHS-Millennium (MP) MOU and/or Business AssociateAgreement and consistent with HIPAA and HITECH policies:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub L. No. 104-191 (Aug 21 1996,codified in scattered sections of title 42 USC (full text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy andSecurity Rules).

- Health Information and Technology for Economic and Clinical Health (HITECH) Act, Title XIII of division Aand Title IV of Division B of the American Recovery and Reinvestment Act of 2009, P.L. No. 111-5, 123 Stat. 226 (Feb 17, 2009) codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.

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.

These procedures will be governed by the VABHS-MP MOU/Business Associate agreement, consistent with HIPAAand HITECH, and monitored by Dr. Halasz in coordination with Dr. Millen.

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.

VA Contractor access is verified through VA Personnel Security before access is granted to any VA contractor. Contracts and contractor access are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the Talent Management System (TMS). All contractors are cleared using VA background investigation process and must obtain the appropriate level of background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

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.

No additional privacy or information security training would be offered specific to the HealthMain® system. Existing VA privacy and information security trainings are deemed to be sufficient. DVA awareness training consists of VA TMS trainings VA Privacy and Information Security Awareness and Rules of Behavior (ROB), number 10176 and VA Privacy and HIPAA training, courses number 10203. The trainings must be completed annually. Once completed, all information system users will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements and consequences for non-compliance; and explain how to report incidents as detailed in VA Handbook 6500: Risk Management Framework For VA Information Systems VA Information Security Program. The awareness program is consistent, continuously updated and required for all employees, including contractors and temporary staff. Dr. Halasz and Dr. Millen will coordinate the training of all VABHS providers and MOVE! counselors.

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

If Yes, provide:

1. *The Security Plan Status,*

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

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

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

No, IOC: March 1, 2023

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.

Yes, the system does use cloud technology. The system is in the process of attaining an ATO. The HealthMain® system utilizes VAEC AWS cloud model Platform as a Service (PaaS).

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

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

N/A

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A

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

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

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

N/A

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

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

N/A
The system does not utilize Robotics Process Automation (RPA)

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Penny M. Lashua 127258

Digitally signed by Penny M. Lashua 127258
Date: 2022.10.17 14:01:31 -04'00'

Privacy Officer, Penny Lashua

Digitally signed by ANDREW VILAILACK
Date: 2022.10.17 15:29:04 -04'00'

Information System Security Officer, Andrew Vilailack

HARRIS KHAN

Digitally signed by HARRIS KHAN
Date: 2022.10.18 16:13:18 -04'00'

Information System Owner, Harris Khan

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).

This pilot will be governed by the MOU and/or Business Associate Agreement between VABHS and Millennium Prevention, Inc and consistent with HIPAA and HITECH policies. VABHS clinicians will refer patients to the pilotand explain the scope of the pilot, consistent with VABHS clinical policies and our MOU/BAA.

The Privacy Act system of records notice (SORN) that covers the information with the HealthMain® is 24VA10A7, Patient Medical Records-VA. 85 FR 52406.

https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

https://www.healthmain.com/privacy/

https://www.healthmain.com/terms/

https://www.healthmain.com/about/

https://www.healthmain.com/welcome/