Privacy Impact Assessment for the VA IT System called:

Remote Patient Monitoring/Home Telehealth - Medtronic (RPM/HT-M)

Veteran Health Administration (VHA)

Office of Connected Care / Telehealth & Scheduling

eMASS ID #2426

Date PIA submitted for review:

10/24/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dennis Lahl	dennis.lahl@va.gov	202-461-7330
Information System Security Officer (ISSO)	Oliver Patague	oliver.patague@va.gov	509-910-2849
Information System Owner	Ellen Hans	ellen.hans@va.gov	703-534-0205

Abstract

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

Remote Patient Monitoring/Home Telehealth - Medtronic (RPM/HT-M).

Medtronic Care Management Services (MCMS) participates in the VA Home Telehealth Program sponsored by VA Office of Connected Care / Telehealth & Scheduling, providing remote care management for Veterans with complex chronic conditions.

The RPM/HT-M system is utilized by the VA to provide a home/remote telehealth monitoring program for Veterans. The system's functions are, on a daily basis and in a secure manner, to remotely acquire specific Veteran health information, via a suite of remote monitoring patient-facing platforms, i.e., devices/peripherals, and deliver to the backend systems which reviews, categorizes, prioritizes, and ultimately presents to the VA Care Coordinator to efficiently monitor the health of a Veteran.

To acquire Veteran health information, a Veteran, typically on a daily basis, answers/addresses a list of health questions (aka Disease Management Protocol or DMP) and vital signs by using one of four modalities noted below. Note - Communication methods include secure cellular, landline or internet connection.

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:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?
IT System Name: Remote Patient Monitoring/Home Telehealth - Medtronic (RPM/HT-M)
Program Office: Office of Connected Care / Telehealth & Scheduling.

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
The RPM/HT-M is utilized by the VA to provide a home/remote telehealth monitoring program for Veterans. The system's functions are, on a daily basis and in a secure manner, to remotely acquire specific Veteran health information. The information is then reviewed, categorized, prioritized, and presented to the VA Care Coordinator to monitor the health of a Veteran.

C. Who is the owner or control of the IT system or project?
VA Owned and non-VA Operated IT system maintained in VAEC-AWS.

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?
Approximately 55,000 Veterans generally with comorbidities.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

Personal Identifiable Information (PII) and Personnel Health Information (PHI) collected in order for VA Care Coordinators to monitor a Veteran's health at home.

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.

The RPM/HT-M system acquires/maintains Veteran PHI and data through a Veteran's completion of an electronic health status questionnaire via multiple proprietary modalities including Commander Flex (CD390), InterVIEW (IOS/Android), LinkView (video) and TeleResponse. RPM/HT-M also acquires/maintains Veteran and limited VA Care Coordinator PII data (for enrollment and patient management purposes) from the VA managed VistA and Oracle Health Cerner Electronic Health Record systems. RPM/HT-M shares PII/PHI data with VA managed VistA and Oracle Health Cerner Electronic Health Record systems. See section 4.1 and 5.1 for more specific information.

G. Is 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?

The information system will reside within VAEC-AWS and will be consistently managed across one or more availability zones.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

RPM/HTH-M has a FIPS 199 categorization of High, has the legal authority to operate under Title 38, United States Code, Sections 501(b) and 304, and collects information under VA SORN 24VA10A7 / 85 FR 62406 – Patient Medical Records – VA.24VA10A7/85 FR 62406 - Patient Medical Records-VA.

I. 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 RPM HT/M system is using cloud technology. The SORN does not require amendment or revision. The SORN for the system covers cloud usage and storage.

4. System Changes

J. Will the completion of this PIA will result in circumstances that require changes to business processes?

Yes.

K. Will the completion of this PIA could potentially result in technology changes?

Yes

Section 1. Characterization of the Information

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

1.1 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. It must also match the information provided in question 3.4 of the PTA.

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

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

Other PII/PHI data elements:

- All geographical subdivisions smaller than a State
  - Street address
  - City
  - Zip code
- All elements of dates
  - Admission date
  - Discharge date
  - Date of death
- Device identifiers and serial numbers
- Any other unique identifier:
  - Gender
  - Marital Status
  - Primary Language

- Secondary Language
- Occupation
- Disability Status
- Allergies
- Data File Number (DFN)
- Electronic Data Interchange Personal Identifier (EDIPI)
- Omnivisor Pro ID number
- Biometric Health data
  - Blood pressure readings (systolic/diastolic)
  - PulseOx Readings (blood oxygen)
  - Heart Rate from both Blood Pressure and PulseOx
  - Glucometer Readings (blood sugar)
  - Weight Scale Readings
  - Spirometer Readings (PEF/FEV1)
  - Pedometer Readings (steps)
  - Thermometer Readings (temperature)
  - Medical Condition Question Responses
  - Mood levels
  - Pain levels

PII Mapping of Components (Servers/Database)

Remote Patient Monitoring/Home Telehealth - Medtronic consists of **five** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that *component* collect PII. The type of PII collected by **Remote Patient Monitoring/Home Telehealth - Medtronic** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
census and survey	Yes	Yes	• Names	Veteran Identification	• Data encrypted in transit and at rest

			• All geographical subdivisions smaller than a State o Street address o City o Zip code • All elements of dates o Birth date o Admission date o Discharge date • Social Security numbers • Device identifiers and serial numbers • Any other unique identifier o Gender o Marital Status o Race o Primary Language o Secondary Language o Occupation o Disability Status o Allergies o Electronic Data Interchang Personal Identifier (EDIPI) o Integrated Control Number (ICN) o Omnivisor Pro ID number		• Access requires management approval and is based on need

rdc-adapter-api.careaware.ehr.gov/v1/medtronic/patient/discretedata/	Yes	Yes	• Any other unique identifier: o Integrated Control Number (ICN) o Biometric Health data ▪ Blood pressure readings (systolic/diastolic) ▪ PulseOx Readings (blood oxygen) ▪ Heart Rate from both Blood Pressure and PulseOx ▪ Glucometer Readings (blood sugar) ▪ Weight Scale Readings ▪ Spirometer Readings (PEF/FEV1) ▪ Pedometer Readings (steps) ▪ Thermometer Readings (temperature) ▪ Medical Condition Question Responses ▪ Mood levels ▪ Pain levels	Veteran Health Status	• Data encrypted in transit and at rest • Access requires management approval and is based on need
hdrclusa.aac.va.gov	Yes	Yes	• Any other unique identifier: o Integrated Control Number (ICN) o Biometric Health data ▪ Blood pressure readings (systolic/diastolic) ▪ PulseOx Readings (blood oxygen) ▪ Heart Rate from both Blood Pressure and PulseOx ▪ Glucometer Readings (blood sugar) ▪ Weight Scale Readings ▪ Spirometer Readings (PEF/FEV1) ▪ Pedometer Readings (steps) ▪ Thermometer Readings (temperature)	Veteran Health Status	• Data encrypted in transit and at rest • Access requires management approval and is based on need

			▪ Medical Condition Question Responses ▪ Mood levels ▪ Pain levels		
mpi-austin.med.va.gov - mpi service	Yes	Yes	• Names • All geographical subdivisions smaller than a State: o Street address o City o Zip code • All elements of dates: o Birth date • Phone numbers; • Electronic mail addresses; • Social Security numbers; • Any other unique identifier: o EDIPI (Electronic Data Interchange Personal Identifier) o Integrated Control Number (ICN) o Gender	Veteran Identification	• Data encrypted in transit and at rest • Access requires management approval and is based on need
vaww.hl7.cns.htr.vaec.va.gov - census service	Yes	Yes	• Names • All geographical subdivisions smaller than a State: o Street address o City o Zip code • All elements of dates: o Birth date • Phone numbers; • Electronic mail addresses; • Social Security numbers; • Any other unique identifier: o EDIPI (Electronic Data Interchange Personal Identifier) o Integrated Control Number (ICN) o Gender	Veteran Identification	• Data encrypted in transit and at rest • Access requires management approval and is based on need

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?
Information received and maintained by the Remote Patient Monitoring/Home Telehealth - Medtronic system consists of identification and biometric data primarily gathered by electronic devices utilized by Veteran's in their homes. The devices vary based on the type of medical condition being monitored. The sources of information are from a combination of devices and tools (i.e. pulse oximeter) which patients use to answer symptomatic questions (aka Disease Management Protocol or DMP) and generate biometric data readings to complete a health check (or status of health). The device and or tools read and record patient biometric data and is then transmitted to the Omnivisor Pro system which can be viewed by VA Client Care Coordinators. Two VA Care Coordinator data elements are also acquired and maintained. Additionally, the RPM/HT-M system and the VA's Electronic Health Records (EHR) system transmit specific Veteran's data to one another as required.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.
Information is acquired from the VA Care Coordinator and the VA's Electronic Health Records (EHR) for Veteran registration, identification, and monitoring.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
The Omnivisor Pro system, per the data acquired from a Veteran, generates a value (and in some cases an alert) based on the parameters set by VA Care Coordinator.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?
Information is primarily collected from both a Veteran via electronic devices, and in a very limited capacity, a VA Care Coordinator. To acquire Veteran health information, a Veteran, typically on a daily basis, answers/addresses a list of health questions (aka Disease Management Protocol or DMP) and vital signs by using one of four modalities noted below. Note - Communication methods include secure cellular, landline or Internet connection.1-Commander Flex (CD390): A physical device, provided to patient, which connects with peripherals record vital type biometric data. 2-InterVIEW (IOS/Android): A mobile application accessible by cell phone, tablet etc. 3-LinkVIEW (video): A physical device that is provided to the Veteran which can connect to peripheral extensions and utilize to record biometric data readings. This option

has video conferencing capabilities.4-TeleResponse (including Vital Sign Relay Device - VSRD): A telephone system whereby Veterans are able to use voice capabilities to record their biometric statistics. The Veteran health information data is securely transmitted through one of several methods including, cellular, landline, or a VA provided modem connection or internet connection. The information collected associated with a VA Care Coordinator is acquired as part of the Veteran enrollment process. Additionally, the RPM/HT-M system and the VA's Electronic Health Records (EHR) system transmit specific Veteran's data to one another as required.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?
All information is collected electronically.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.
1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.
Hashing algorithms and checksums are utilized when sending and verifying information integrity. The system verifies that data has been sent from an active device ID.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?
RPM/HT-M does not use a commercial aggregator of information.

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.
RPM/HT-M operates under the legal authority of Title 38, United States Code, Section 501(b) and 304 and collects information under the System of Record of VA SORN 24VA10A7 / 85 FR 62406 - Patient Medical Records - VA.

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

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

Principle of Purpose Specification: 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:
RPM/HT-M, to assist with a Veteran's healthcare, collects and maintains only the required Personally Identifiable Information (PII) and Personal Health Information (PHI) information from both a Veteran and the VA's Care Coordinator. If this data were accessed or inadvertently released to unauthorized parties or the public, it could result in personal, financial, and/or emotional harm to the individual.

Mitigation:
RPM/HT-M implements a considerable number of security mechanisms and mitigations including, but not limited to, the following:

- Data is encrypted in transit and at rest.
- Servers are maintained behind VA firewalls.
- Administrative access is provisioned with least user privilege and reviewed at least quarterly.
- Annual security awareness training is required.
- Separate test, development, and production environments.
- Change Management process.
- Application and infrastructure vulnerability scanning and remediation management.
- Disaster Recovery and Incident Response plans in place and assessed annually.
- Anti-virus/malware prevention.
- Physical and environmental data center controls (managed by VA).
- Subject to the VA's Authority-to-Operate (ATO) security management and control structure.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
'Source' from Section 1.1: Veterans or Dependents • Names* • All geographical subdivisions smaller than a State o Street address o City o Zip code • All elements of dates o Birth date* o Admission date o Discharge date o Date of death • Phone numbers • Electronic mail addresses • Social Security numbers* • Device identifiers and serial numbers • Any other unique identifier o Gender o Marital Status o Race o Primary Language o Secondary Language o Occupation o Disability Status o Allergies o Integrated Control Number (ICN)* o Data File Number (DFN) o Electronic Data Interchange Personal Identifier (EDIPI)* o Omnivisor Pro ID number o Biometric Health data* ▪ Blood pressure readings (systolic/diastolic) ▪ PulseOx Readings (blood oxygen) ▪ Heart Rate from both Blood Pressure and PulseOx ▪ Glucometer Readings (blood sugar) ▪ Weight Scale Readings ▪ Spirometer Readings (PEF/FEV1) ▪ Pedometer Readings (steps) ▪ Thermometer Readings (temperature) ▪ Medical Condition Question Responses ▪ Mood levels ▪ Pain levels	Identify, enroll, communicate, product delivery, and tracking a Veteran's health status	*Data elements sent to Veterans Health Administration - Electronic Health Record (EHR) system(s) for Veteran's health status

'Source' from Section 1.1: VA Care Coordinator • Names ○ Electronic Data Interchange Personal Identifier (EDIPI)	Management of a Veteran's health status	NA

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?
All RPM/HT-M associated data collected is transmitted to and maintained within the Omnivisor Pro system. The Omnivisor Pro system does not utilize any tools to analyze data but rather generates alerts based on defined settings established by the VA Care Coordinator.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
Veteran PHI and PII is acquired/maintained within the RPM/HT-M system. This information is available to VA Care Coordinators via MCMS's Omnivisor Pro application/database which also communicates some data elements with the VA managed VistA and Oracle Health Cerner Electronic Health Record systems.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?
RPM/HT-M encrypts data at rest and in transit, along with logical access (strong authentication) controls and a VA user/patient access provisioning process.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
RPM/HT-M encrypts data at rest and in transit.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
All personnel with access participate in annual privacy training and are required to sign the rules of behavior (ROB) which describes what behaviors are allowed and not allowed on a VA system. Access requires management approval and is based on the principal of least privilege. Additionally, RPM/HT-M implements a considerable number of security mechanisms and

mitigations including, but not limited to, the following: Data is encrypted in transit and at rest. Servers are maintained behind VA firewalls. Administrative access is provisioned with least user privilege and reviewed at least quarterly. Annual security awareness training is required. Separate test, development, and production environments. Change Management process. Application and infrastructure vulnerability scanning and remediation management. Disaster Recovery and Incident Response plans in place and tested annually. Anti-virus/malware prevention. Physical and environmental data center controls (managed by VA). Subject to the VA's Authority-to-Operate (ATO) security management and control structure.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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.

2.4a How is access to the PII determined?

Data gathered and stored in the RPM/HT-M system is used to by VA Clinical Care Coordinators to ascertain the current health status of a Veteran. System Administrative access requires management approval, is based on the principal of least privilege, and reviewed at least quarterly. All personnel with access participate in annual privacy training and are required to sign the rules of behavior (ROB) which describes what behaviors are allowed and not allowed on a VA system. Any inappropriate use of information will be reported to the VA Program Manager.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes via the MCMS Access Control Standard Operating Procedure (SOP).

2.4c Does access require manager approval?

Yes, all MCMS Administrative access requires manager approval.

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

Yes. Administrative access is monitored through the Solarwinds Event Manager (SEM) auditing tool.

2.4e Who is responsible for assuring safeguards for the PII?

All RPM/HT-M personnel.

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*

Source	Data elements
Veterans or Dependents	• Names • All geographical subdivisions smaller than a State ○ Street address ○ City ○ Zip code • All elements of dates ○ Birth date ○ Admission date ○ Discharge date ○ Date of death • Phone numbers • Electronic mail addresses • Social Security numbers • Device identifiers and serial numbers • Any other unique identifier ○ Gender ○ Marital Status ○ Race ○ Primary Language ○ Secondary Language ○ Occupation ○ Disability Status ○ Allergies ○ Integrated Control Number (ICN) ○ Data File Number (DFN) ○ Electronic Data Interchange Personal Identifier (EDIPI) ○ Omnivisor Pro ID number ○ Biometric Health data ▪ Blood pressure readings (systolic/diastolic) ▪ PulseOx Readings (blood oxygen) ▪ Heart Rate from both Blood Pressure and PulseOx ▪ Glucometer Readings (blood sugar) ▪ Weight Scale Readings ▪ Spirometer Readings (PEF/FEV1) ▪ Pedometer Readings (steps)

	▪ Thermometer Readings (temperature) ▪ Medical Condition Question Responses ▪ Mood levels ▪ Pain levels
VA Employees	• Names • Any other unique identifier: ○ Electronic Data Interchange Personal Identifier (EDIPI)

3.2 How long is information retained?

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

Health information stored on electronic media is maintained for 75 years following its most recent update. The data is systematically and securely destroyed after this duration in strict adherence to the protocols outlined in the VA Handbook 6500.1 - Electronic Media Sanitization. This handbook mandates the destruction of all data assigned to a high-security categorization. Per the SORN, 24VA10A7 / 85 FR 62406, Policies and Practices for Retention and Disposal of Records, "In accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6." rcs10-1.pdf (va.gov).

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. 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. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes. RPM/HT-M records are retained in accordance with the Department of Veterans Affairs Record Control Schedule 10-1, Item Number 6000.2 “Electronic Health Record”. http://www.va.gov/vhapublications/RCS10/rcs10-1.pdf.

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

Retention Schedule: Electronic Medical Records, (EHR) - 75-yearsSeries: VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.2b Disposition Authority: (N1–15–02–3, Item 3).

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.
Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.
https://www.va.gov/vapubs/search_action.cfm?dType=1

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.
The RPM/HT-M system does not use PII or live data for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

Principle of Minimization: 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:
The longer the timeframe that RPM/HT-M system data is kept increases the risk for potential compromise or breach.

Mitigation:
RPM/HT-M strictly adheres to the Records Management Schedule in order to ensure that records are not maintained longer than necessary. System Administrative access requires management approval, is based on the principal of least privilege, and reviewed at least quarterly. All personnel with access participate in annual privacy training and are required to sign the rules of behavior (ROB) which describes what behaviors are allowed and not allowed on a VA system. The data is also stored in VA data centers where a layered security infrastructure exists that is complemented by physical and environmental safeguards.

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***
Veterans' Health Administration - VistA systems / Electronic Health Record (EHR)	Veteran health check	• Names • All geographical subdivisions smaller than a State ○ Street address ○ City ○ Zip code • All elements of dates ○ Birth date ○ Phone Numbers • Electronic mail addresses • Social Security numbers • Electronic mail addresses • Any other unique identifier ○ Electronic Data Interchange Personal Identifier (EDIPI) ○ Integrated Control Number (ICN) ○ Gender ○ Biometric Health data ▪ Blood pressure readings (systolic/diastolic) ▪ PulseOx Readings (blood oxygen) ▪ Heart Rate from both Blood Pressure and PulseOx ▪ Glucometer Readings (blood sugar) ▪ Weight Scale Readings ▪ Spirometer Readings (PEF/FEV1) ▪ Pedometer Readings (steps) ▪ Thermometer Readings (temperature) ▪ Medical Condition Question Responses ▪ Mood levels ▪ Pain levels	HL7 (Health Link)

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*
VA Census Survey	Identify Veteran for health check	• Names • All elements of dates: ○ Birth date ○ Admission date ○ Discharge date • Social Security numbers • Device Identifiers • Any other unique identifier: ○ Electronic Data Interchange Personal Identifier (EDIPI) ○ Integrated Control Number (ICN) ○ Omnivisor Pro ID number	HL7 (Health Link)

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk:
RPM/HT-M system data may be disclosed to unauthorized individuals which could result information being misused.

Mitigation:
The principle of need-to-know is strictly adhered to by RPM/HT-M personnel. Only personnel with a business need are allowed access to the system.

Section 5. External Sharing/Receiving and Disclosure

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

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

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal

mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: 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***
Veterans' Health Administration Oracle Health Cerner system / Electronic Health Record (EHR)	Veteran health check	• Names • All elements of dates ○ Birth date ○ Phone Numbers • Social Security numbers • Any other unique identifier ○ Electronic Data Interchange Personal Identifier (EDIPI) ○ Integrated Control Number (ICN) ○ Biometric Health data ▪ Blood pressure readings (systolic/diastolic) ▪ PulseOx Readings (blood oxygen)	Interagency Agreement DOD DHA VA National MEDCOI ISA - ID 733 E-5290	Group Encrypted Transport VPN - IPsec tunnel utilizing Joint Security Architecture (JSA) across MedCOI (Medical Community of Interest)

		▪ Heart Rate from both Blood Pressure and PulseOx ▪ Glucometer Readings (blood sugar) ▪ Weight Scale Readings ▪ Spirometer Readings (PEF/FEV1) ▪ Pedometer Readings (steps) ▪ Thermometer Readings (temperature) ▪ Medical Condition Question Responses ▪ Mood levels ▪ Pain levels		
HTH-Med Assessing system - Hub Device - Cellular; Kore Networking	Remote healthcare monitoring for Veteran	• Names • Any other unique identifier ○ Biometric Health data ▪ Blood pressure readings (systolic/diastolic) ▪ PulseOx Readings (blood oxygen) ▪ Heart Rate from both Blood Pressure and PulseOx ▪ Glucometer Readings (blood sugar) ▪ Weight Scale Readings ▪ Spirometer Readings (PEF/FEV1) ▪ Pedometer Readings (steps) ▪ Thermometer Readings (temperature) ▪ Medical Condition Question Responses ▪ Mood levels ▪ Pain levels	MOU/ISA - VA Contract #: VA791-17-D-0004; SORN #: 24VA10A7 /85 FR 62406 - Patient Medical Records-VA	Site-to-Site Connection: Cellular; HSA hardware chip encryption supporting FIPs 140-2 encryption

HTH-Med Assessing system: Hub Device - Plain Old Telephone System (POTS)	Remote healthcare monitoring for Veteran	• Names • Any other unique identifier ○ Biometric Health data ▪ Blood pressure readings (systolic/diastolic) ▪ PulseOx Readings (blood oxygen) ▪ Heart Rate from both Blood Pressure and PulseOx ▪ Glucometer Readings (blood sugar) ▪ Weight Scale Readings ▪ Spirometer Readings (PEF/FEV1) ▪ Pedometer Readings (steps) ▪ Thermometer Readings (temperature) ▪ Medical Condition Question Responses ▪ Mood levels ▪ Pain levels	VA Contract #: VA791-17-D-0004; SORN #: 24VA10A7 /85 FR 62406 - Patient Medical Records-VA	Plain old Telephone System; HSA hardware chip encryption supporting FIPs 140-2 encryption
HTH-Med Assessing system: TeleResponse - Interactive Voice Response (IVR)	Remote healthcare monitoring for Veteran	• Names • Any other unique identifier ○ Biometric Health data ▪ Blood pressure readings (systolic/diastolic) ▪ PulseOx Readings (blood oxygen) ▪ Heart Rate from both Blood Pressure and PulseOx ▪ Glucometer Readings (blood sugar) ▪ Weight Scale Readings ▪ Spirometer Readings (PEF/FEV1) ▪ Pedometer Readings (steps) ▪ Thermometer Readings (temperature) ▪ Medical Condition Question Responses ▪ Mood levels ▪ Pain levels	VA Contract #: VA791-17-D-0004; SORN #: 24VA10A7 /85 FR 62406- Patient Medical Records-VA	Telephony System

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

Follow the format below:

Privacy Risk:
RPM/HT-M system data may be inadvertently shared with external and/or unauthorized individuals which could result information being misused.

Mitigation:
Outside organizations are required to provide their own level of security controls such as access control, authentication, and user logs to prevent unauthorized access. Additional mitigations include:
- All personnel with access to RPM/HT-M system data are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior (ROB) annually.
- RPM/HT-M adheres to the information security requirements instituted by the VA Office of Information Technology (OIT).

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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (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?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a 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, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.
Veterans are asked if they want to enroll in the Home Telehealth Program by their VA Care Coordinator. Confirming they are willing to participate in the program justifies the gathering of the information for RPM/HT-M system. In addition, a notice was provided via a system of records notice published in the Federal Register: Patient Medical Records-VA SORN (24VA10A7). https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
See Appendix A-6.1, *Enrollment Agreement.

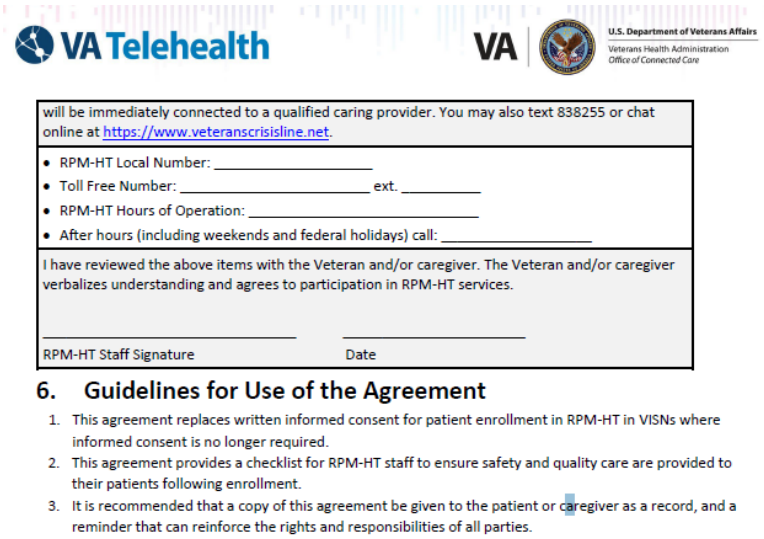
6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.
See RPM-HT Enrollment Agreement below.

VA Telehealth

VA U.S. Department of Veterans Affairs Veterans Health Administration Office of Connected Care

5. RPM-HT Enrollment Agreement

This Enrollment Agreement documents RPM-HT Program information and other educational materials have been given to _____ (Name of Veteran patient and/or caregiver). It confirms the information below has been given and is understood and agreed to by the Veteran and/or Caregiver.
RPM-HT programs ensure that all relevant state and federal health-related privacy/confidentiality regulations are met to safeguard the protected health information of all RPM-HT Veterans.
The rights and responsibilities of participation in a VHA RPM-HT program have been fully explained and are understood, including the right to refuse telehealth services at any time, and including the fact that refusal to participate in telehealth by a Veteran will not limit or adversely affect further access to VA health care services.
The Veteran and/or caregiver were fully informed about VHA complaint procedures.
Answers to the disease-specific questions and vital signs administered to the Veteran are required every day from the Veteran unless explicitly otherwise instructed, as charted in the Electronic Health Record (EHR). Lack of active participation may impact success in the program and may result in disenrollment from RPM-HT.
In the event of technology/equipment malfunction, the Veteran and/or caregiver should contact the RPM-HT staff.
Veterans will use the technology as directed in provided instructions. This includes, but is not limited to, using the power cord provided with the device and following directions for safe use of batteries as detailed in instructions provided with any devices.
Upon disenrollment from the RPM-HT program the telehealth In-Home Messaging Device (IHMD) will be returned to the Denver Logistics Center (DLC). The RPM-HT staff will order a Retrieval Kit for the Veteran and the Veteran will use the kit with the postage-paid label to return the In-Home Messaging Device (IHMD), as well as cables and any other equipment indicated by the care coordinator. The Veteran can ask RPM-HT staff for assistance with returning their technology/equipment.
The RPM-HT program is provided with the sole intent of monitoring Veterans with stable chronic disease and cannot cover acute exacerbations (flare ups) or deteriorations. Neither the equipment, nor the care coordinator can provide a route whereby emergency care can be provided. The Veteran and/or caregiver should call 911 if they need to access immediate emergency medical attention.
In the event of an emotional crisis associated with risk of self-harm, VHA has a 24 hour/7 day a week suicide prevention hotline that can be accessed by dialing or texting 988 and then Press 1, or you may call 1-800-273-TALK (8255) and Press 1 for Veterans. The Veteran and/or caregiver



will be immediately connected to a qualified caring provider. You may also text 838255 or chat online at https://www.veteranscrisisline.net.

- RPM-HT Local Number: _____
- Toll Free Number: _____ ext. _____
- RPM-HT Hours of Operation: _____
- After hours (including weekends and federal holidays) call: _____

I have reviewed the above items with the Veteran and/or caregiver. The Veteran and/or caregiver verbalizes understanding and agrees to participation in RPM-HT services.

_____ _____

RPM-HT Staff Signature Date

6. Guidelines for Use of the Agreement

1. This agreement replaces written informed consent for patient enrollment in RPM-HT in VISNs where informed consent is no longer required.
2. This agreement provides a checklist for RPM-HT staff to ensure safety and quality care are provided to their patients following enrollment.
3. It is recommended that a copy of this agreement be given to the patient or caregiver as a record, and a reminder that can reinforce the rights and responsibilities of all parties.

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.
Yes. Veteran's do have the opportunity and right to decline to provide information. Veteran patients are asked if they want to enroll in the VA Home Telehealth Program by the VA Care Coordinators. Participating in the VA Home Telehealth Program requires Veterans to provide information directly to the RPM/HT-M system by using medical devices or telephones located in their home. If a Veteran does not want to provide information, they only need to dis-enroll from the Home Telehealth program.

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.
Yes, Veteran's do have the right to consent to particular uses of the information. Veterans are notified as part of the enrollment process how their information will be used. Enrollment constitutes consent. Participating in the VA Home Telehealth Program requires Veterans to provide information directly to the RPM/HT-M system. If a Veteran does not want to provide information, they only need to dis-enroll from the program.

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: 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:
Veterans who provide information to RPM/HT-M system may not know how their information is being shared and used internal to the Department of Veterans Affairs and may be unaware that the RPM/HT-M relays information through intermediary sites.

Mitigation:
This PIA and the VA Home Telehealth enrollment process serve to notify individuals of how information is handled by the RPM/HT-M system.

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?
These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***
VHA Directive 1605.01 outlines the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request For a Copy 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 System 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.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

The RPM/HT-M system is not exempt from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?
The RPM/HT-M system is a Privacy Act system.

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
VHA Directive 1605.01 outlines the rights of the Veterans to amend to their records. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1. 579.The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.
The SORN 24VA10A7 and VHA Notice of Privacy Practices informs individuals how to file an amendment request with VHA.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
Formal redress is addressed in SORN 24VA10A7 and VHA Notice of Privacy Practices informs individuals how to file an amendment request with VHA.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those

risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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:
Information provided by the Veteran may be inadvertently inaccurate and the Veteran may not be aware and/or know how to correct the information.

Mitigation:
VA Care Coordinators review all information input into the RPM/HT-M system. If a Veteran wants to access their information, they may ask their VA Clinical Care Coordinator to provide their information. They may also be directed to the Release of Information Department where they can request access to their information.

Section 8. Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system, and are they documented?
These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?
Administrator procedures are in place for the two primary types of users that access the RPM/HT-M system, MCMS System Administrators and VA Client Care Coordinators.

(1) MCMS System Administrators access the RPM/HT-M system in order to maintain the functionality of the system, which requires elevated privileges and is associated with their position. This access is granted through the VA onboarding process via the ePAS (electronic Permission Access System) process. Only users with a need-to-know and a valid business need

are granted access. Administrative access requires management approval, provided on a least privilege basis, and is reviewed quarterly.

(2) VA Client Care Coordinators are granted access to the system in order to review patient records and provide support to the Veterans. Access is granted and set up in the Omnivisor Pro system by VA Lead Care Coordinators.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?
No users from other agencies have access to the system.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.
(1) MCMS System Administrators access the RPM/HT-M system in order to maintain the functionality of the system, which requires elevated privileges and is associated with their position. (2) VA Client Care Coordinators are granted access to the system in order to review patient records and provide support to the Veterans.

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.
The RPM/HT-M system is maintained by Medtronic Care Management Services (MCMS) who are contracted by the VA Office of Connected Care/VHA Telehealth Services to provide support and assistance to the program. The contract award number is 36C79123D0001. The contract award was for a base period of two years and six option periods. The contract is reviewed each year and renewed by way of a contract amendment. All MCMS personnel involved in the operations of the RPM/HT-M system complete the VA Security Clearance process. The following documents are reviewed and signed annually by each team member, (1) Non-Disclosure Agreement (2) Contractor Rules of Behavior. Additionally, team members must also complete, an annual basis the VHA Privacy and HIPAA Focused Training and VA Privacy and Information Security Awareness Training.

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

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.

This question is related to privacy control AR-5, Privacy Awareness and Training.
All personnel involved in the operations of the RPM/HT-M program have completed the initial and annual security and privacy training required by the contract. Users with elevated privileges have undergone training unique to their specific role. Team members must also complete the VA's Talent Management System (TMS) Privacy and HIPAA Focused Training and Privacy and Information Security Awareness Training. Medtronic Care Management Services (MCMS) also requires all employees to complete annual MCMS based HIPAA and Security trainings.

8.4 Has Authorization and Accreditation (A&A) been completed for the system? No

8.4a If Yes, provide:

1. *The Security Plan Status: <<ADD ANSWER HERE>>*
2. *The System Security Plan Status Date: <<ADD ANSWER HERE>>*
3. *The Authorization Status: <<ADD ANSWER HERE>>*
4. *The Authorization Date: <<ADD ANSWER HERE>>*
5. *The Authorization Termination Date: <<ADD ANSWER HERE>>*
6. *The Risk Review Completion Date: <<ADD ANSWER HERE>>*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): <<ADD ANSWER HERE>>*

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***
Anticipated for 3/1/2024. Moderate Categorization.

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?
If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*
RPM/HT-M is a COTS system and will utilize VAEC-AWS.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of*

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

<<ADD ANSWER HERE>>

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.

<<ADD ANSWER HERE>>

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.

<<ADD ANSWER HERE>>

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).

<<ADD ANSWER HERE>>

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2023.11.13 15:13:52 -05'00'

Privacy Officer, Dennis Lahl

OLIVER PATAGUE Digitally signed by OLIVER PATAGUE
Date: 2023.11.01 15:23:36 -07'00'

Information Systems Security Officer, Oliver Patague

ELLEN HANS (Affiliate) Digitally signed by ELLEN HANS (Affiliate)
Date: 2023.11.03 09:43:39 -04'00'

Information Systems Owner, Ellen Hans

APPENDIX A-6.1

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

VA SORN 24VA10A7/85 FR 62406 - Patient Medical Records-VA Patient Medical Records–VA.
a. Effective Date: 10/02/2020
b. Link to Printed Version: 2020-21426.pdf (govinfo.gov)

System of Records Notice
VHA Handbook 1605.4 *Notice of Privacy Practices*, October 7, 2015
(https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147)

*Enrollment Agreement

5. RPM-HT Enrollment Agreement

This Enrollment Agreement documents RPM-HT Program information and other educational materials have been given to _____ (Name of Veteran patient and/or caregiver). It confirms the information below has been given and is understood and agreed to by the Veteran and/or Caregiver.
RPM-HT programs ensure that all relevant state and federal health-related privacy/confidentiality regulations are met to safeguard the protected health information of all RPM-HT Veterans.
The rights and responsibilities of participation in a VHA RPM-HT program have been fully explained and are understood, including the right to refuse telehealth services at any time, and including the fact that refusal to participate in telehealth by a Veteran will not limit or adversely affect further access to VA health care services.
The Veteran and/or caregiver were fully informed about VHA complaint procedures.
Answers to the disease-specific questions and vital signs administered to the Veteran are required every day from the Veteran unless explicitly otherwise instructed, as charted in the Electronic Health Record (EHR). Lack of active participation may impact success in the program and may result in disenrollment from RPM-HT.
In the event of technology/equipment malfunction, the Veteran and/or caregiver should contact the RPM-HT staff.
Veterans will use the technology as directed in provided instructions. This includes, but is not limited to, using the power cord provided with the device and following directions for safe use of batteries as detailed in instructions provided with any devices.
Upon disenrollment from the RPM-HT program the telehealth In-Home Messaging Device (IHMD) will be returned to the Denver Logistics Center (DLC). The RPM-HT staff will order a Retrieval Kit for the Veteran and the Veteran will use the kit with the postage-paid label to return the In-Home Messaging Device (IHMD), as well as cables and any other equipment indicated by the care coordinator. The Veteran can ask RPM-HT staff for assistance with returning their technology/equipment.
The RPM-HT program is provided with the sole intent of monitoring Veterans with stable chronic disease and cannot cover acute exacerbations (flare ups) or deteriorations. Neither the equipment, nor the care coordinator can provide a route whereby emergency care can be provided. The Veteran and/or caregiver should call 911 if they need to access immediate emergency medical attention.
In the event of an emotional crisis associated with risk of self-harm, VHA has a 24 hour/7 day a week suicide prevention hotline that can be accessed by dialing or texting 988 and then Press 1, or you may call 1-800-273-TALK (8255) and Press 1 for Veterans. The Veteran and/or caregiver

will be immediately connected to a qualified caring provider. You may also text 838255 or chat online at https://www.veteranscrisisline.net.
• RPM-HT Local Number: _____ • Toll Free Number: _____ ext. _____ • RPM-HT Hours of Operation: _____ • After hours (including weekends and federal holidays) call: _____
I have reviewed the above items with the Veteran and/or caregiver. The Veteran and/or caregiver verbalizes understanding and agrees to participation in RPM-HT services. _____ _____ RPM-HT Staff Signature Date

6. Guidelines for Use of the Agreement

1. This agreement replaces written informed consent for patient enrollment in RPM-HT in VISNs where informed consent is no longer required.
2. This agreement provides a checklist for RPM-HT staff to ensure safety and quality care are provided to their patients following enrollment.
3. It is recommended that a copy of this agreement be given to the patient or caregiver as a record, and a reminder that can reinforce the rights and responsibilities of all parties.

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices