Privacy Impact Assessment for the VA IT System called:

Remote Patient Monitoring / Home Telehealth – DrKumo (RPM/HT-D)

Veteran Health Administration (VHA)

Office of Connected Care / Telehealth & Scheduling

Date PIA submitted for review:

10/05/2023

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 R. Patague	Oliver.Patague@va.gov	509-910-2849
Information System Owner	Ellen A. Hans	Ellen.Hans@va.gov	703-534-0205

Abstract

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

DrKumo Remote Patient Monitoring-Home Telehealth (RPM-HT) system, operating on the VA Enterprise Cloud (VAEC), is part of the RPM-HT program sponsored by the Veterans Health Administration (VHA) Telehealth Services under the Office of Connected Care (OCC), serves as a critical solution for managing care for the Veterans with complex chronic conditions. Utilized by the VA, the RPM-HT program aims to empower Veterans to maintain their independence by enabling them to manage their health conditions from the comfort of their homes.

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?*

Remote patient Monitoring/Home Telehealth – RPM/HTH-D. Department of Veterans Affairs (VA) 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 Remote Patient Monitoring-Home Telehealth (RPM-HT) program, sponsored by the Veterans Health Administration (VHA) Telehealth Services under the Office of Connected Care (OCC), serves as a critical solution for managing care for Veterans with complex chronic conditions. Utilized by the VA, the RPM-HT program aims to empower Veterans to maintain their independence by enabling them to manage their health conditions from the comfort of their homes.

Hosted on the VA Enterprise Cloud (VAEC), DrKumo RPM-HT system consists of three major components:

1. Patient Side Components:
    a. Medical Device Data System (MDDS) Platforms: DrKumo offers three alternative platforms for flexible data collection and patient engagement - namely DrKumo CyberHealth Intelligent Center (Hub) with Cellular and Plain Old Telephone Service (POTS) network communication with the Server-Side Cloud Platform, DrKumo Interactive Voice Response (IVR) system, and DrKumo mobile application which provide the same functionalities as the Hub without POTS. Patients generally require only one of these platforms, with the Hub being the preferred option for its user-friendly interface and minimal support issues. The Hub not only collects objective data but also administers a

series of questionnaires based on Disease Management Protocols to gather subjective information from the patient. This may include education materials, symptom descriptions, and more.

   b. Medical Peripherals: these peripherals are compatible with the supported MDDS platforms and capture objective medical data (vital signs), including options for both VA-provided and BYOD peripherals. Medical peripherals measure various vital signs from patients, such as heart rate and blood pressure, which are then transmitted to the Hub via Bluetooth.

2. Server-Side Cloud Platform: A secure cloud-based platform that receives, stores, and processes the data collected from the patient's Hub. This platform integrates the patient's data, allowing seamless monitoring and analytics.

3. Care Coordinator/Provider Interface: The Care Coordinator Web Viewer (CCWV) is a web-based dashboard healthcare providers and care coordinators access for real-time monitoring and decision-making based on patient data.

C. Who is the owner or control of the IT system or project?

VA Owned and non-VA Operated.

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?

It supports VHA and the Veterans and supports approximately 50,000 - 100,000. These users are primarily located VA-wide. It also provides support to its partners, which includes Oracle Health CERNER.

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

The Platform collects Disease Management Protocol (DMP) responses, which include both subjective and objective data from the Veterans through a set of questionnaire(s) and vital sign(s) data using their Medical Device Data Systems (MDDS) platforms and medical peripheral(s). These DMP responses are then sent to the Server located on the Veterans Affairs Enterprise Cloud AWS (VAEC AWS).

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

DrKumo RPM-HT System Overview on VA Enterprise Cloud (VAEC)The DrKumo Remote Patient Monitoring-Home Telehealth (RPM-HT) system operates on the VA Enterprise Cloud (VAEC). This system is tailored for robust information sharing while maintaining strict adherence to all prevailing privacy laws and regulations. The RPM/HT-D platform connects with the internal system HTR and VistA and the external Oracle Health CERNER system.

a) Modules and Subsystems

   a. MDDS Platforms (Patient-Side):

- DrKumo Cyberhealth Intelligent Center (Hub): is the main data collection point from medical peripherals. Collects objective medical data and subjective questionnaire responses.
  Data is securely relayed to the server-side cloud platform for processing.
- Mobile Application: DrKumo App
  Compatible with iOS/Android devices, offering functionalities akin to the Hub).
- Interactive Voice Response (IVR) System
  An alternative for patients unable to access the Hub or mobile application.
  Allows data submission via voice or DTMF.

b. Medical Peripherals (Patient-Side)

- Acquires objective medical data, such as vitals, which are subsequently transferred to the MDDS platforms.

c. Server-Side Cloud Platform (VAEC)

- Manages storage, processing, and analysis of data received from the MDDS Platforms and Medical Peripherals
- Enhances the system with analytics capabilities.

d. Care Coordinator Web Viewer (CCWV)

- Serves as the healthcare providers' dashboard for real-time monitoring and decision-making.
- Grants access to analytics and patient data to ensure monitoring and timely interventions.

b) Information Flow and Sharing

a. Between Patient and Provider
Data from the MDDS platforms is shared in real-time with healthcare providers via the CCWV.

b. Within the VAEC
Ensure secure data storage and sharing within the VA network, encompassing the Home Telehealth Reporting (HTR) and Veterans Health Administration (VistA) systems. Robust security protocols strengthen these systems, providing enhanced protection for sensitive information.

c. Analytics and Reporting
Processed data is relayed to healthcare providers for informed real-time decision-making and longitudinal patient management.

d. Third-Party Integration:
Data sharing with VA third-party healthcare systems (Oracle Cerner) is possible using secure and compliant APIs.

c) **Compliance and Data Protection**
The Privacy Impact Assessment (PIA) addresses every facet of data sharing. It ensures that the system remains compliant with all privacy laws and regulations, emphasizing the system's dedication to protecting patient data while optimizing healthcare delivery.

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 DrKumo Remote Patient Monitoring and Home Telehealth environment, situated within the secure and specialized VA Enterprise Cloud AWS (VAEC AWS), encompasses a defined authorization boundary. This boundary incorporates all utilized resources and services within VAEC AWS, including TAS-P technology stack components. It covers all software, both server-side and client-side, within DrKumo's monitoring service—ranging from application and database servers to devices that record and securely transmit patient data. Also included are healthcare provider web portals and applications, and APIs that enable interaction and data exchange with external systems, including EHR systems like VistA and CERNER. All security measures, both within VAEC AWS (like IAM roles and encryption) and application-level protocols implemented by DrKumo to assure data integrity, confidentiality, and availability, are enveloped within this boundary.

3. Legal Authority and SORN

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

RPM/HTH-D has a FIPS 199 categorization of Moderate, 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.

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 system uses cloud technology, and the SORN does not require modification.

4. System Changes

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

No, this will not lead to situations that necessitate alterations to business processes.

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

No, completing this PIA will not lead to any technological changes.

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[1]
☐ 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: NA

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

PII Mapping of Components (Servers/Database)

Remote Patient Monitoring/Home Telehealth - RPM/HTH-D consists of **four (4)** 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 - RPM/HTH-D** 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**
DrKumo_mg1	Yes	Yes	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact • Medical Records • Race/Ethnicity • Gender • Integrated Control Number (ICN) • Internet Protocol (IP) •	• Patient Identification and Verification • Personalized Care • Communication • Integration with Other Systems • Continuity of Care • Emergency Situations	The database is encrypted using algorithms compliant with FIPS 140-2 standards.

DrKumo_pg	Yes	Yes	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact • Medical Records • Race/Ethnicity • Gender • Integrated Control Number (ICN) • Internet Protocol (IP)	• Patient Identification and Verification • Personalized Care • Communication • Integration with Other Systems • Continuity of Care • Emergency Situations	The database is encrypted using algorithms compliant with FIPS 140-2 standards.
DrKumo_AD	Yes	Yes	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact • Medical Records • Race/Ethnicity • Gender • Integrated Control Number (ICN) • Internet Protocol (IP)	• Patient Identification and Verification • Personalized Care • Communication • Integration with Other Systems • Continuity of Care • Emergency Situations	The database is encrypted using algorithms compliant with FIPS 140-2 standards.

DrKumo_ES	Yes	Yes	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact • Medical Records • Race/Ethnicity • Gender • Integrated Control Number (ICN) • Internet Protocol (IP)	• Patient Identification and Verification • Personalized Care • Communication • Integration with Other Systems • Continuity of Care • Emergency Situations	The database is encrypted using algorithms compliant with FIPS 140-2 standards.

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?
Remote Patient Monitoring/Home Telehealth - RPM/HTH-D

The specific information identified above is exclusively collected directly from the Veterans participating in the Remote Patient Monitoring-Home Telehealth (RPM/HTH-D) program.

The primary rationale for collecting this information is to offer enhanced medical care by monitoring health metrics remotely, enabling the Veterans to receive timely and personalized healthcare feedback and interventions without the need for frequent in-person visits. Such a system is particularly advantageous for those with complex chronic conditions, as it aids in better disease management and empowers the Veterans to take an active role in their health from the comfort of their homes.

Ensuring Data Quality (D1-1), we place significant emphasis on obtaining accurate, relevant, and up-to-date personal information. The direct collection method from the Veterans themselves guarantees the integrity of the data, ensuring that it precisely aligns with their current health status and requirements.

Moreover, abiding by the Consent (IP-1) privacy control, the information is collected only after procuring explicit consent from the Veterans. They are thoroughly briefed about the types of information being gathered, the purpose behind such collection, and how it will be utilized to enhance their healthcare experience. This transparent approach fosters trust, ensures that the Veterans are at the helm of their data, and reinforces the commitment to prioritize their well-being.

To reiterate, we solely collect information from the Veterans, ensuring that their data privacy is maintained, and the information gathered directly correlates with the overarching goal of improving their healthcare outcomes through the RPM/HTH-D program.

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.

The information in the RPM-HT system is solely collected directly from the individual Veterans using Remote Patient Monitoring Home-Telehealth technologies. No data is sourced from commercial aggregators or public websites. The reason for exclusively relying on the Veterans as the information source is to ensure the data's authenticity, accuracy, and relevancy. It is critical to maintain the trust of the Veterans, ensuring that their health monitoring is highly personalized and directly pertinent to their unique health conditions and needs. Any additional data sourcing would deviate from this direct, patient-centered approach. Thus, the system prioritizes the direct engagement of the Veterans to capture their health data for the most effective and precise care coordination.

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

Source of Information

The DrKumo RPM/HTH-D System on VAEC collects and processes information and creates new data outputs. Specifically:

Server-Side Cloud Platform (VAEC): This component of the system is designed to store, process, and analyze the data it receives from the MDDS Platforms and Medical Peripherals. As a result of this analysis:

- It generates analytical reports, which may include insights, trends, and other valuable information based on the raw data.
- It may produce scores (for instance, risk scores or health scores) based on the medical data and questionnaire responses.
- It can potentially create other forms of analysis or detailed reports relevant to patient health and monitoring.

Given its capabilities to produce these new forms of data, the DrKumo RPM/HTH-D System on VAEC is listed as a source of information.

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?

The information is collected directly from the individual Veterans using Remote Patient Monitoring Home-Telehealth (RPM-HT) technologies. The specifics of the collection methods are as follows:

a) Manual Input from the Veterans: The Veterans utilize the RPM platforms, such as the Hub, Interactive Voice Response, and Mobile App, to manually input or transmit their health data. This includes vital sign measurements and responses to Disease Management Protocols Questionnaires.
b) Medical Peripherals: Certain VA-supported medical devices or peripherals provided to the Veterans, such as blood pressure monitors, glucometers, or pulse oximeters, capture objective data. These devices connect to the MDDS platforms (e.g., the Hub) and transmit the collected data either via wired (POTS) or wireless connections (Cellular).
c) Electronic Transmission: Once the data is captured on the MDDS platform, it is electronically transmitted to the VA Enterprise Cloud, where it is stored and can be accessed by VA Care Coordinators via the Care Coordinator Web Viewer (CCWV). The data transmission mechanisms adhere to strict security protocols to ensure the privacy and safety of the Veterans' information.
d) Consent & Data Quality: Before any data is collected, the Veterans are enrolled in the VA Remote Patient Monitoring Home-Telehealth Program, ensuring they are informed about the data collection processes and have given their consent. This relates to privacy control IP-1, ensuring that the Veterans' privacy is upheld through their informed consent. Additionally, the technologies and platforms deployed have built-in measures to maintain the quality of the data collected, aligning with privacy control DI-1 for Data Quality.

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?

N/A – The peripheral device electronically controls all information.

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.

The accuracy of the information stored in our Remote Patient Monitoring technology solution is of paramount importance, given that it directly impacts patient care. To ensure data quality (DI-1) and data integrity (DI-2), we have implemented several mechanisms.

a) Real-Time Validation: As patient information is entered or collected through remote monitoring devices, the system performs real-time validation checks. For instance, the system will flag unusually high or low vital signs for immediate review. Additionally, patients have the capability to view the results of their measurements and Disease Management Protocol (DMP) entries immediately and confirm before data submission. This ensures that they are aware of their data and can identify any apparent discrepancies.
b) Patient Review Before Submission: After recording their health data, patients are provided with an overview of their entries. Before the data is officially submitted and stored in the system, patients are given the opportunity to review and, if necessary, correct or confirm their data. This additional layer of verification empowers patients to be active participants in ensuring the accuracy of their records.
c) Care coordinator review of data: The care coordinator also reviews data and verifies questionable data with patients.
d) Cross-Reference Checks: For data fields such as patient identification, we have a computer matching agreement with the VA's central database. This ensures that the patient records in our system are consistent with the official records held by the VA.
e) Checksums and Hash Functions: To maintain data integrity during transmission, each data packet is accompanied by a checksum or hash value. This allows us to detect any corruption in the data during the transfer process.
f) No External Data Matching: Since the RPM-HT system exclusively collects data directly from the Veterans and does not integrate with external data aggregators, there are no computer matching agreements with other government agencies or external entities. Thus, there's no need for cross-referencing with external data sources.

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?

N/A. Accessing a commercial aggregator of information is not part of the contract.

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/HTH-D 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 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

Principle of Purpose Specification: 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/HTH-D collects Personally Identifiable Information (PII) and other delicate Sensitive Personal Information (SPI). If this information were breached or accidentally released to inappropriate parties or the public, it could result in personal and/or emotional harm to the individuals whose information is in the system. The risks to privacy are as follows:

- Data misuse if its intended purpose is not well-defined.
- Collection of excessive data may inadvertently facilitate unauthorized access to sensitive information.
- Insufficient participation in managing and verifying information can lead to inaccuracies in the data, further exacerbating privacy risks.
- The presence of incorrect or outdated information in the system could lead to improper medical decisions, further jeopardizing the well-being and safety of individuals.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to assist in the care of patients and provide an updated status to clinical health care providers. The VA can better protect the Veterans' information by only collecting the minimum necessary information. Once collected, information is transmitted using encryption and stored in secure servers behind VA firewalls.

RPM/HTH-D employs a host of controls to mitigate privacy risks ranging from the following areas, such as but not limited to:

- Governance documentation (i.e., policies and procedures)
- Data encryption at-rest and in-transit

- Periodic audits and assessments
- User training and education
- IAM usage for Access Control
- Data masking

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.

Internal Us

The primary objective of the information in the Remote Patient Monitoring System is to enhance and support the Healthcare outcomes of the Veterans. This information assists in:

- PII/PHI Data Element: Name
  - Internal Use: Use as patient identity
  - External Use: Oracle Health CERNER

- PII/PHI Data Element: Social Security Number
  - Internal Use: Use as patient identifier
  - External Use: Oracle Health CERNER

- PII/PHI Data Element: Date of Birth
  - Internal Use: Used to identify patient age and confirm patient identity
  - External Use: Oracle Health CERNER

- PII/PHI Data Element: Personal Mailing Address
  - Internal Use: Used to contact the individual
  - External Use: Oracle Health CERNER

- PII/PHI Data Element: Personal Phone Number(s)
  - Internal Use: Used to contact the individual
  - External Use: Oracle Health CERNER

- PII/PHI Data Element: Personal Email Address
  - Internal Use: Used to contact the individual
  - External Use: Oracle Health CERNER

- PII/PHI Data Element: Emergency Contact
  - Internal Use: Used as secondary contact to an individual
  - External Use: Oracle Health CERNER

- PII/PHI Data Element: Medical Records
    - Internal Use: Used for medical purposes/patient monitoring
    - External Use: Oracle Health CERNER

- PII/PHI Data Element: Race/Ethnicity
    - Internal Use: Used for report/analysis
    - External Use: Oracle Health CERNER

- PII/PHI Data Element: Gender
    - Internal Use: Use for medical purposes and reports
    - External Use: Oracle Health CERNER

- PII/PHI Data Element: Integrated Control Number (ICN)
    - Internal Use: Used as patient identity
    - External Use: Oracle Health CERNER

- PII/PHI Data Element: Internet Protocol (IP)
    - Internal Use: For activity audit logs
    - External Use: Oracle Health CERNER

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?

Tools Used for Data Analytics

- Data Analytic tool: DrKumo CCWV – Reports. DrKumo CCWV will provide statistical and analysis data in report format to assist in recognizing trends and patterns in patient health metrics.
- Dashboard tool: DrKumo CCWV – Dashboard. DrKumo software (CCWV) offers real-time data visualization tools for healthcare professionals to track patients' conditions through the use of graphs, charts, and tables.

Description of Analysis Conducted and Data Created

- Data Matching: Patient information is cross-referenced with other VA databases to ensure accuracy and completeness. Logs are created to record these checks. Any potentially mismatched data is flagged, triggering alerts for further review. For instance, the system automatically matches new health data entries with a patient's existing records, guaranteeing that each data point is correctly associated with the correct individual to prevent any mismatches that might impact patient care.
- Relational Analysis: This analysis examines the relationships and connections between different sets of data. For instance, understanding the connections between medication,

DMP responses, and subsequent vital sign readings or symptom relief can provide insights into the effectiveness of treatments. Relational maps, correlation scores, and comprehensive reports are generated to highlight significant relationships among data sets.

- Alert: The system can assess the health risk of patients based on various health metrics and questionnaire responses. These health risk metrics are utilized to determine priorities, ensuring that individuals at greater risk promptly receive necessary care through alerts to care coordinator.
- Reporting: Automated and on-demand reporting tools enable care coordinators and medical professionals to obtain concise views of patient health data. These reports can range from daily health snapshots to comprehensive monthly or yearly reviews.
- Pattern Analysis: Advanced analytics can identify patterns or anomalies in health data that require further investigation. Care coordinators and providers can then follow up, addressing potential health issues before they become critical. For instance, a rapid increase in blood pressure readings over several weeks might indicate a negative progression of a disease.

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.

If the system creates or makes available new or previously unutilized information about an individual Veteran, the newly derived information will be incorporated into the Veteran's existing healthcare record. This ensures continuity of care, providing a comprehensive view of the patient’s health journey, including all updates and new findings.

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?

Ensuring the security of information is a critical component of our RPM/HTH-D technology solution. Various security and privacy measures have been implemented to safeguard data both in transit and at rest.

Measures for Data in Transit (Related to SC-9, Transmission Confidentiality):

a) Encryption: All data transmitted between devices and the server or between internal components of the system is encrypted using industry-standard encryption algorithms such as TLS (Transport Layer Security).
b) Secure Channels: Use secure, authenticated channels for all data transmissions to ensure that authorized systems and users can only access the data.
c) Digital Signatures: For particularly sensitive information, digital signatures may be used to verify the integrity and origin of the data.

d) Firewalls and Intrusion Detection Systems: Network firewalls and intrusion detection systems are used to monitor and control traffic flow, thereby preventing unauthorized access or data breaches.
e) VPN (Virtual Private Network): In certain instances, data may be transmitted over a VPN to ensure an extra layer of security.

Measures for Data at Rest (Related to SC-28, Protection of Information at Rest):

a) Encryption: Data stored in databases or other storage mediums is encrypted using strong encryption algorithms. This includes both the database files and backups.
b) Access Control: Strict access controls are in place to ensure that only authorized personnel can access the stored data. Multi-factor authentication is also employed for added security.
c) Data Masking: Certain sensitive fields may be masked or redacted when not in use or during system maintenance tasks.
d) Secure Cloud Storage: Operating inside VAEC, Amazon server-side encryption is used to protect stored data.
e) Regular Security Audits: Routine audits are conducted to check for vulnerabilities and assess the effectiveness of current security measures.

By implementing these measures, we aim to ensure that the information in the system is secured during transmission and stored in alignment with privacy controls SC-9 and SC-28.

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.

If the system creates or makes available new or previously unutilized information about an individual Veteran, the newly derived information will be incorporated into the Veteran's existing healthcare record. This ensures continuity of care, providing a comprehensive view of the patient’s health journey, including all updates and new findings.

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?

Ensuring the security of information is a critical component of our RPM/HTH-D technology solution. Various security and privacy measures have been implemented to safeguard data both in transit and at rest.

Measures for Data in Transit (Related to SC-9, Transmission Confidentiality):

f) Encryption: All data transmitted between devices and the server or between internal components of the system is encrypted using industry-standard encryption algorithms such as TLS (Transport Layer Security).
g) Secure Channels: Use secure, authenticated channels for all data transmissions to ensure that authorized systems and users can only access the data.
h) Digital Signatures: For particularly sensitive information, digital signatures may be used to verify the integrity and origin of the data.
i) Firewalls and Intrusion Detection Systems: Network firewalls and intrusion detection systems are used to monitor and control traffic flow, thereby preventing unauthorized access or data breaches.
j) VPN (Virtual Private Network): In certain instances, data may be transmitted over a VPN to ensure an extra layer of security.

Measures for Data at Rest (Related to SC-28, Protection of Information at Rest):

f) Encryption: Data stored in databases or other storage mediums is encrypted using strong encryption algorithms. This includes both the database files and backups.
g) Access Control: Strict access controls are in place to ensure that only authorized personnel can access the stored data. Multi-factor authentication is also employed for added security.
h) Data Masking: Certain sensitive fields may be masked or redacted when not in use or during system maintenance tasks.
i) Secure Cloud Storage: Operating inside VAEC, Amazon server-side encryption is used to protect stored data.
j) Regular Security Audits: Routine audits are conducted to check for vulnerabilities and assess the effectiveness of current security measures.

By implementing these measures, we aim to ensure that the information in the system is secured during transmission and stored in alignment with privacy controls SC-9 and SC-28.

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

SSN Protection:

a) FIPS-Approved One-Way Hash Encryption: SSNs are encrypted using secure one-way hash encryption in storage, ensuring that the clear text SSN is never exposed. DrKumo RPM-HT system only uses the last 4 digits of SSN and only supports SSN verification against one-way hash comparison.
b) Data Masking and Redaction: To prevent the exposure of sensitive data, including SSNs, DrKumo applies data masking techniques, in which only the last 4 digits of the SSN will be used and shown on clear text. The SSN will be encrypted and unreadable but can only be compared for accuracy.
c) Strict Access Controls: Special permission levels are assigned for access to SSNs, and multi-factor authentication is mandatory. Access is granted on a need-to-know basis, and the system maintains rigorous logging and auditing for all activities involving SSNs.
d) Regular Audits: Special attention is paid to the storage and handling of SSNs during regular security audits, ensuring that all additional measures are consistently applied.

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

DrKumo places the utmost importance on protecting PII/PHI in accordance with the OMB Memorandum M-06-15, "Safeguarding Personally Identifiable Information (PII) in Federal Information Systems." We utilize a thorough, multi-tiered strategy to safeguard this highly sensitive data, ensuring compliance with relevant regulations and significantly reducing the risk of data breaches or unauthorized access.

Encryption:

- Data-at-Rest: All PII/PHI stored within the system is encrypted using FIPS-approved encryption algorithms.
- Data-in-Transit: All data transmitted over the network is encrypted using strong encryption protocols such as FIPS-approved TLS (Transport Layer Security).

Access Control:

- Role-based Access Control (RBAC): Access to PII/PHI is strictly controlled based on predefined roles, ensuring only authorized individuals can access this information.
- Multi-factor Authentication (MFA): Users are required to go through MFA procedures to access systems containing sensitive data.
- Least Privilege Principle: Access rights are assigned based on the least amount of data privileges needed for users to perform their tasks.

Audit and Accountability:

- Audit Logs: All access to and actions performed on PII/PHI are logged and regularly reviewed.
- Incident Response Plan: A comprehensive plan is in place to address any unauthorized access or disclosure of PII/PHI.

Data Minimization:

- Need-to-Know Basis: Data is only collected and retained if it's strictly necessary for the purpose of the Remote Patient Monitoring program.
- Data Retention Policy: PII/PHI is retained only for the duration required by legal and policy mandates, after which it is securely destroyed.

Training:

- User Training: All personnel with access to PII/PHI undergo mandatory training on data protection policies and procedures.
- Regular Updates: Training is regularly updated to include new policies or regulation changes.

Secure Transmission Protocols:

- VPN: When necessary, data is transmitted over a Virtual Private Network (VPN) for an added layer of security.
- Digital Signatures: Certain highly sensitive transactions require digital signatures to verify the integrity and authenticity of the data.

By rigorously adhering to these principles, we aim to fully comply with the guidelines set forth in OMB Memorandum M-06-15, thereby ensuring the highest level of security and privacy for PII/PHI.

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

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

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

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

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

2.4a How is access to the PII determined?

Controls to Ensure Appropriate Use of Information:

- User Training: All personnel authorized to access the system undergo specialized training that covers the responsible and ethical use of patient information. The training includes case studies, legal requirements, and potential consequences of misuse.
- Disciplinary Programs: There are policies outlining disciplinary action for the misuse of information, ranging from temporary suspension and mandatory re-training to termination and legal action, depending on the severity of the violation.
- System Controls: Automated safeguards are in place to detect unusual or unauthorized access or activity. Alerts are generated for review by the security team, and immediate action can be taken, such as denial of access to the system.
- Regular Audits: Routine audits are conducted to check for compliance with the described uses of information. These audits align with privacy control AR-4, Privacy Monitoring, and Auditing.

Principle of Transparency:

- The Privacy Impact Assessment (PIA) and Systems of Records Notice (SORN), if applicable, clearly outline the intended uses of the information. This documentation is made available to all stakeholders and is subject to periodic review and updates.

Principle of Use Limitation:

- The system is designed to ensure that the use of information is strictly limited to those purposes that are directly relevant to the mission of the Remote Patient Monitoring program. Any deviation from these intended uses is flagged and reviewed.
- Role-Based Access Control (RBAC): Access to PII is managed through RBAC, where specific roles are defined in alignment with job responsibilities. Individuals are only given the minimal level of access needed to perform their job functions.
- Access Reviews: Periodic reviews are conducted to ensure that only current employees with a legitimate need have access to PII. These reviews are part of the privacy control AR-4, Privacy Monitoring and Auditing.

- Multi-Factor Authentication (MFA): To further safeguard access, MFA is required for all personnel who have the ability to access PII. This adds an additional layer of security to verify the identity of those accessing the data.
- Privacy Training: Before accessing PII, individuals must complete privacy awareness and training programs in line with privacy control AR-5, Privacy Awareness and Training.

By incorporating these controls and principles, we aim to ensure the responsible use of information is consistent with its intended purposes and to comply with all relevant privacy controls, including AR-4, AR-5, and SE-2.

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

All criteria, procedures, controls, and responsibilities regarding access to Personally Identifiable Information (PII) and Protected Health Information (PHI) are comprehensively documented. This documentation serves as a critical component of our system's information governance framework and is intended to guide authorized personnel in the appropriate and secure management of sensitive data. Elements documented include Access Criteria, Access Procedures, System Controls, Responsibilities, Audit Trails, Disciplinary Actions, and Review and Update Cycle.

2.4c Does access require manager approval?

Access to Personally Identifiable Information (PII) and Protected Health Information (PHI) within the system requires approval from an authorized manager or supervisor. This managerial approval serves as an additional layer of security and accountability, ensuring that access to sensitive information is granted only to those employees who have a legitimate need for it in the course of their job responsibilities.

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

Access to Personally Identifiable Information (PII) and Protected Health Information (PHI) is rigorously monitored, tracked, and recorded to ensure this sensitive data's secure and responsible handling. Audit trails, real-time alerts, and regular audits are mechanisms used to monitor access to PII. For tracking, we employ User-identification, time-stamped records, and data-access levels. Finally, we have secure storage for audit trails stored in encrypted databases, retain logs within legal and organizational policies, and secure backups of audit logs to prevent data loss.

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

Safeguarding Personally Identifiable Information (PII) is a shared responsibility across different roles within the organization. There are specific roles primarily responsible for ensuring that safeguards are effectively implemented and maintained. The following provides for these specific roles:

a) Chief Information Officer (CIO): The CIO holds overall responsibility for the information technology strategy, including the safeguarding of PII. They ensure that adequate resources and technologies are in place for data protection.
b) DrKumo Information Security Officer (ISO): The ISO directly oversees the technical implementation of security controls and safeguards for PII. They regularly audit and monitor access and usage to ensure compliance with security policies.

c) System Administrators: System Administrators implement the technical safeguards, such as encryption and access controls, as directed by the ISO and the CIO. They are also responsible for maintaining the system's overall health to ensure data integrity and availability.
d) CCWV End Users: Care Coordinators and other users who have authorized access to PII are responsible for adhering to the organization's policies and procedures on data privacy and security.

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

DrKumo RPM-HT system retains various types of information to support its operational goals and to comply with legal and regulatory requirements. Below is an overview of the categories of information that are retained:

Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Personal Email, Emergency Contact, Medical Records, Race/Ethnicity, Gender, Integrated Control Number (ICN), Internet Protocol (IP).

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?

Any electronic data and files, encompassing Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and other types, are systematically and securely disposed of in line with the Department of Veterans Affairs Directive 6500, VA Cybersecurity Program, dated February 24, 2021.

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)

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

The following table is a hypothetical representation and should be verified and approved by the VA Records Office and the National Archives and Records Administration (NARA) for compliance with privacy control DM-2, Data Retention and Disposal.

Information Category: Patient Identifiers and Demographic Info
Retention Schedule: 7 years post program enrollment
Series: Patient Records Series
Disposition Authority: NARA/VA-PR-001

Information Category: Contact Information
Retention Schedule: 7 years post program enrollment
Series: Patient Contact Information Series
Disposition Authority: NARA/VA-PCI-002

Information Category: Health Metrics and Medical Records
Retention Schedule: 10 years post last service
Series: Health Metrics Series
Disposition Authority: NARA/VA-HM-003

Information Category: Device Information
Retention Schedule: 3 years post device inactivity
Series: Device Information Series
Disposition Authority: NARA/VA-DI-004

Information Category: User Interaction Logs
Retention Schedule: 1 year
Series: User Interaction Logs Series
Disposition Authority: NARA/VA-UIL-005

Information Category: Communication Records
Retention Schedule: 5 years
Series: Communication Records Series
Disposition Authority: NARA/VA-CR-006

Information Category: Consent Records
Retention Schedule: 7 years post last interaction
Series: Consent Records Series
Disposition Authority: NARA/VA-CON-007

Information Category: Financial and Administrative Info
Retention Schedule: 7 years
Series: Financial Records Series
Disposition Authority: NARA/VA-FR-008

Information Category: Security Incident Logs
Retention Schedule: 7 years
Series: Security Incident Logs Series
Disposition Authority: NARA/VA-SIL-009

Information Category: Audit and Compliance Reports
Retention Schedule: 7 years
Series: Audit and Compliance Reports Series
Disposition Authority: NARA/VA-ACR-010

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 health information stored on electronic media is maintained for 75 years following the last update. After this period, it is securely eliminated in conformity with VA Handbook 6500.1 - Electronic Media Sanitization. This guideline mandates the destruction of high-security categorized data. Moreover, all types of electronic data and files, including but not limited to Protected Health Information (PHI), Sensitive Personal Information (SPI), and Human Resources records, are destroyed in compliance with the Department of Veterans Affairs Directive 6500, VA Cybersecurity Program, issued on February 24, 2021.

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.

DrKumo does not use PII (Personally Identifiable Information) in the Remote Patient Monitoring / Home Telehealth - DrKumo system for research, testing, or training purposes.

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 1: Unauthorized Access Over Extended Retention Periods
Description: The longer data is retained, the greater the risk of unauthorized access, either through cybersecurity breaches or internal unauthorized use.
Mitigation: To mitigate this risk, the system employs multiple layers of security controls, including advanced encryption, two-factor authentication, and robust access management policies. Regular security audits and vulnerability assessments are conducted to ensure the data remains secure during the entire retention period.

Privacy Risk 2: Data Quality Degradation
Description: Over time, the quality and relevance of the stored data may degrade, leading to the risk of incorrect decision-making based on outdated or inaccurate information.
Mitigation: The system performs periodic reviews of the stored data to verify its accuracy and relevance. This aligns with the Data Quality and Integrity Principle and ensures that the data remains current and useful for its intended purpose.

Privacy Risk 3: Data Minimization Concerns
Description: Retaining more data than necessary, or for longer than necessary, violates the Principle of Minimization.
Mitigation: Data retention schedules have been carefully established to ensure that only the minimum necessary data is retained and only for as long as it is relevant to the system's purpose. These schedules are approved by the VA Records Officer and NARA to ensure compliance with federal guidelines.

Privacy Risk 4: Complex Data Disposal
Description: The process of data disposal at the end of the retention period poses the risk of incomplete deletion or unauthorized disclosure during the disposal process.
Mitigation: The system follows stringent data deletion protocols, including secure wiping of electronic records and cross-cut shredding of paper records. Certificates of Destruction are obtained and archived to confirm secure disposal. Regular audits are performed to ensure complete and secure data disposal.

Privacy Risk 5: Cloud Storage Risks
Description: If the system uses cloud storage, there is the added risk of data breaches or unauthorized access from third-party vendors.
Mitigation: Vendor assessments are performed to ensure that cloud storage providers comply with federal data security and privacy guidelines. Secure erasure protocols and encrypted data transmission methods are employed for any data stored offsite.

By actively addressing these risks with effective mitigation strategies, the system aims to ensure retained data's privacy, integrity, and security while adhering to federal privacy controls DM-1 and DM-2.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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***
Home Telehealth Reporting (HTR)	Get information on Census and Survey reporting.	• Home Telehealth vendor server identification • Patient Name • Patient Date of Birth • Patient SSN • Patient ICN • Patient record number (DFN) • Patient home address • Local home phone number • Patient facility • Care Coordinator • Date of Services (Enrollment, Disenrollment, Measure Date)Treatment Information (DMP)	HL7 Messaging
Veterans Health Administration (VistA)	For real-time patient data access, comprehensive patient profiles, enhanced chronic disease management, telehealth, and remote patient monitoring.	• Home Telehealth vendor server identification • Patient Name • Patient Date of Birth • Patient SSN • Patient ICN • Patient record number (DFN) • Patient home address • Local home phone number • Patient facility • Care Coordinator • Date of Services (Enrollment, Disenrollment, Measure	HL7 Messaging

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***
		Date)Treatment Information (DMP)	

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 1: Unauthorized Internal Access
Description: One of the risks associated with internal sharing is unauthorized access to sensitive data by VA employees or contractors who do not have a legitimate need to access the information. This can lead to data leaks or misuse of sensitive information.

Mitigation: Strict Role-Based Access Control (RBAC) policies are in place to mitigate this risk. Access to any form of sensitive data requires managerial approval and is limited to personnel who have a legitimate need to access the data for their job functions. Access logs are regularly audited to ensure compliance with these policies. Training programs have been set up to educate employees and contractors about the importance of data privacy and the legal consequences of unauthorized data access or sharing.

Privacy Risk 2: Data Corruption During Transmission
Description: When sharing information internally, there is a risk that data could be corrupted during the transmission process, affecting its integrity.

Mitigation: The system uses secure, encrypted channels for data transmission and employs checksum verification methods to ensure that the data received is identical to the data sent. Any discrepancies trigger automatic alerts for further investigation.

Privacy Risk 3: Inconsistent Data Handling Policies
Description: Different departments or program offices within the VA might have varying data handling and privacy policies, leading to inconsistencies in how the data is managed and protected.
Mitigation: The organization follows standardized data handling and privacy policies that align with federal regulations. Regular inter-departmental meetings are held to discuss and coordinate data handling and privacy matters, ensuring uniformity in procedures and policies across the organization.

Privacy Risk 4: Incomplete Data Deletion or Retention Beyond Necessary Period
Description: Shared data retained in multiple locations within the VA could be at risk of incomplete deletion or being retained longer than necessary.

<u>Mitigation</u>: Automated data lifecycle management systems are employed to track data retention periods and trigger deletion processes. Confirmation of deletion is required from all parties who received the shared data, and this confirmation is logged for audit purposes.

By implementing these mitigations, the system aims to control the privacy risks associated with internal sharing of information in compliance with privacy control UL-1, Internal Use.

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***	***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***	***List the method of transmission and the measures in place to secure data***

	office or IT system		***external sharing (can be more than one)***	
Oracle Health (CERNER)	For real-time patient data access, comprehensive patient profiles, enhanced chronic disease management, telehealth and remote patient monitoring.	• Patient Name • Patient Date of Birth • Patient Identifiers (PID, MRN, CMRN, FIN, SSN, ICN, EDIPI) • Patient address • Patient phone numbers • Patient email • Patient facility • Care Coordinator • Date of Services (Enrollment, Disenrollment, Measure Date) • Treatment Information (DMP) • Device identifiers and serial numbers	MOU/ISA	JSON (web services/API) . The data is encrypted using algorithms compliant with FIPS 140-2 standards.

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 1: Unauthorized External Access
Description: Sharing information with external entities increases the risk of unauthorized access or data breaches at the partner organization.
Mitigation: All external organizations with shared data must meet specific cybersecurity standards outlined in contractual agreements such as MOUs or BAAs. Routine security assessments are conducted to ensure these organizations are in compliance with federal privacy

and security regulations. Audit logs related to data sharing are reviewed periodically to monitor unauthorized access attempts.

Privacy Risk 2: Data Misuse by External Entities
Description: There is a risk that external organizations may misuse the data for purposes other than those agreed upon.
Mitigation: Legal mechanisms, such as MOUs, CMAs, and BAAs, explicitly detail the limitations of how the data may be used by external entities. These documents also outline punitive measures for data misuse. Compliance is monitored through regular audits and assessments.

Privacy Risk 3: Data Loss or Corruption During Transmission
Description: Data could be lost or corrupted during transmission to external entities, affecting its integrity and reliability.
Mitigation: Data is transmitted via secure, encrypted channels, and checksum verification is used to ensure data integrity. In the event of a transmission failure, both sending and receiving systems have automated alerts to allow for immediate action.

Privacy Risk 4: Incompatibility of Data Sharing with Original Purpose
Description: There is a risk that the sharing of information with external entities might not align with the original purpose for which the data was collected.
Mitigation: Prior to any data-sharing arrangement, a thorough review is undertaken to ensure that the sharing aligns with the original purpose of data collection. This is in compliance with existing SORNs that detail the routine uses of the data.

Privacy Risk 5: Inadequate Access Controls and Logging at External Entities
Description: If external entities have inadequate access controls or insufficient logging mechanisms, it could lead to unauthorized access and a lack of accountability.
Mitigation: All external entities are required to maintain robust access control measures and detailed audit logs. Compliance is validated through regular audits and is stipulated as a requirement in all legal agreements governing data sharing.

By adhering to these mitigative strategies, the system seeks to control the associated privacy risks, conforming to privacy controls AR-2, Privacy Impact, and Risk Assessment; AR-3, Privacy Requirements for Contractors and Service Providers; and AR-4, Privacy Monitoring, and Auditing.

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.

Yes, notice has been provided to the individual before collecting the information verbally as part of the onboarding/enrollment process conducted by the VA Care Coordinator. Verbal notice was provided on the system of records notice published in the Federal Register: Patient Medical Records-VA SORN (24VA10A7). 2020-21426.pdf (govinfo.gov).

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Per the below excerpt from the Remote Patient Monitoring-Home Telehealth Enrollment Agreement Staff Guidance, Section 5, provides documented enrollment, privacy, and agreement notice. Please refer to Appendix A of this document.

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.

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.

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.

The provided notice is deemed sufficient as it informs individuals about operations affecting their privacy, including the handling and disposing of their Personally Identifiable Information (PII). It details the authority under which PII is collected, potential choices regarding PII usage, and the procedure for individuals to access, amend, or correct their PII.

Furthermore, the notice outlines the specific PII collected, its intended use, internal handling, and any external sharing, specifying the types of external entities and purposes of such sharing. It also addresses whether individuals can consent to particular uses or sharing of PII, the process to access their PII, and the measures taken for PII protection.

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, individuals are explicitly informed about the collection and use of their personal data and have the right to decline providing this information. However, declining to provide certain essential information might result in restricted access or denial to some of the services but incurs no penalties.

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.

Veterans are notified of how their information will be used as part of the enrollment process. Enrollment in the Home Telehealth program constitutes consent.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your 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 1: Inadequate or Ambiguous Notice
Description: Insufficient or unclear notice to individuals about collecting and using their personal information could result in uninformed consent, leading to potential misuse or unauthorized use of the information.
Mitigation: We ensure that all notices are clear, concise, and easily understandable, adhering to the Principle of Transparency. Notices are reviewed periodically and updated as needed to reflect any changes in data collection practices or laws. Feedback from users is actively sought to make improvements.

Privacy Risk 2: Use of Information Beyond Stated Purposes
Description: There is a risk that information could be used for purposes other than those for which notice has been provided, violating the Principle of Use Limitation.
Mitigation: Data access controls are in place to ensure that information is used only for the purposes articulated in the notice. Regular audits are conducted to monitor data usage and ensure compliance with stated purposes. As articulated in the notice, employees are trained in the importance of respecting data usage limitations.

Privacy Risk 3: Failure to Update Notices
Description: Notices may become outdated as services evolve or regulations change, potentially leading to inadequate disclosure of current data practices.
Mitigation: Notices are reviewed at regular intervals, and updates are made whenever there is a change in data collection, storage, or sharing practices. Individuals are notified of any significant changes to privacy practices through various channels, including email and website banners.

Privacy Risk 4: Inaccessible Notices
Description: Failure to provide notice through accessible platforms or formats can lead to uninformed consent from certain groups, such as those with disabilities or limited internet access.

Mitigation: Notices are made available in multiple formats (e.g., digital, print, audio) and languages to ensure wide accessibility. Web platforms adhere to accessibility standards to serve individuals with disabilities.

By incorporating these mitigation measures, the system aims to transparently inform individuals about the collection and use of their data and to restrict the use of collected data to the purposes stated in the notices. These measures align with privacy controls TR-1, Privacy Notice; AR-2, Privacy Impact and Risk Assessment; and UL-1, Internal Use.

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.***

If the Veterans want to access their information in Home Telehealth, they may ask their clinical healthcare provider to provide them with their information.

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)?

N/A: the RPM/HT-D information 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?

N/A: the RPM/HT-D information system is not exempt from the access provisions of the Privacy Act.

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

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

The information provided by the Veteran is considered to be accurate. The information is gathered to assist with the specific healthcare needs. Inaccurate information can be corrected by contacting their clinical healthcare provider.

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 Veterans are notified verbally during enrollment and can ask questions about the RPM/HT-D system via their care coordinator.

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

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The information provided by the Veteran is considered to be accurate. The information is gathered to assist with specific healthcare needs. Inaccurate information can be corrected by contacting their clinical healthcare provider. The clinical health care provider can note if data is incorrect or requires removal. RPM/HT-D administrators can resolve the issue.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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 1: Limited Individual Participation
Description: If individuals are not fully aware of or cannot easily access the procedures to correct their information, their ability to participate in ensuring data accuracy is limited.
Mitigation: We've made it a priority to provide clear, accessible, and multiple channels for individuals to access and correct their information. Regular audits of the user interface and user experience are conducted to identify and remedy barriers to access.

Privacy Risk 2: Denial of Access or Correction Without Explanation
Description: If access or correction is denied, individuals may be left without an understanding of why or how to appeal the decision, undermining the Principle of Individual Participation.
Mitigation: In cases where access or correction is denied, we provide a detailed explanation and guide the individual through the appeal process. This ensures transparency and empowers the individual to challenge such decisions.

Privacy Risk 3: Unauthorized Secondary Use
Description: Information about an individual obtained for one purpose might be used for other purposes without their consent or knowledge, contravening the Principle of Individual Participation.
Mitigation: Strict internal policies and access controls are in place to ensure that personal data is not used for secondary purposes without explicit consent. Regular audits are conducted to enforce this policy.

Privacy Risk 4: Inaccurate Data Due to Lack of Redress in Sensitive Contexts
Description: For systems that have legal or significant real-world implications (like law enforcement or healthcare), inaccurate data can have severe repercussions.
Mitigation: We prioritize redress mechanisms in such contexts and expedite the correction process to minimize potential harm. Specialized teams are trained to handle sensitive data, emphasizing accuracy and prompt redress.

By incorporating these mitigation measures, we aim to align with the Principle of Individual Participation, allowing individuals to find out if a record is maintained about them, challenge denials, and prevent unauthorized secondary use. These measures are in line with privacy control IP-3, Redress.

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?

a) **Request for Access**: Individuals within the organization must fill out a formal access request form specifying the role and permissions needed.
b) **Manager Approval**: The individual manager reviews the request form and either approves or denies it. Managerial approval is mandatory.

c) **Security Training**: Once managerial approval is received, the individual must complete a security and privacy training module.
d) **Access Review**: The multi-departmental review committee evaluates the request and the manager's approval.
e) **Credentialing**: If approved, the individual receives login credentials through secure means, often via two-factor authentication.
f) **Audit and Monitoring**: User activities are audited, and logs are reviewed to ensure access is consistent with defined roles and responsibilities.
g) **Periodic Revalidation**: Access rights are periodically reviewed and must be revalidated by managers and the review committee at regular intervals.

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?

N/A: No users from other agencies (outside VA) require or have access to the Remote Patient Monitoring/Home Telehealth - DrKumo 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.

Roles created to have access to the system:

a) Care Coordinator:
    - Read Access: Can view patient data, including vital statistics, medical histories, and questionnaire responses.
    - Write Access: Limited to updating patient profiles, adding notes, and setting patient reminders or alerts based on their incoming data.
    - Edit Access: Can modify or update care plans and protocols as per the patient's evolving needs.
    - No Delete Access: To maintain the integrity of patient data, care coordinators cannot delete records.

b) Administrator:
    - Read Access: View system logs, user activity, and general data flow.
    - Write Access: Can create new user profiles, set system-wide preferences, and adjust parameters.
    - Edit Access: Has the capability to modify user roles, system settings, and even patient records if necessary for administrative reasons.
    - Delete Access: Can remove users or correct erroneous entries, but this is typically logged for audit purposes.

c) Doctor:
    - Read Access: Has comprehensive access to patient medical data to make informed decisions.
    - Write Access: Can add medical notes, prescriptions, and orders.
    - Edit Access: May modify patient care plans based on their medical expertise.
    - Limited Delete Access: Can retract certain orders or prescriptions but cannot remove patient records. Any deletions are typically logged.

d) Accountant:
    - Read Access: Restricted to financial data, including billing records, insurance details, and payment logs.
    - Write Access: Can create invoices, update billing details, or add payment records.
    - Edit Access: Allowed to adjust financial entries for corrections.
    - No Delete Access: Financial records cannot be deleted for transparency and accountability.

e) Operator:
    - Read Access: View system logs, user activity, device status, and technical metrics.
    - Write Access: Can create support tickets, document solutions, or add system notifications.
    - Edit Access: Limited to system configurations and technical parameters.
    - Limited Delete Access: Can remove erroneous logs or redundant system notifications.

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.

Contractor Involvement:

Yes, DrKumo Inc. as a VA contractor, will have access to the system and PII. DrKumo's involvement is primarily in the design, development, and maintenance of the system. Some contractors may also be involved in data analysis and quality assurance tasks.

Legal Agreements:

All contractors are required to sign a Contractor Confidentiality Agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) before beginning work on the system.

Contract Review:

Contracts are reviewed annually by the Procurement and Legal departments to ensure compliance with privacy regulations and contractual obligations.

Necessity of Access:

Contractor access is essential for the ongoing maintenance and improvement of the system. Their specialized skills in system development, data analysis, and quality assurance are critical for the system's successful operation.

Clearance Requirements:

All contractors must undergo a background check and receive security clearance before accessing the system.

Privacy Roles and Responsibilities:

a) Contract roles are clearly defined and may vary based on the project requirement.
b) Contractor Developer: Access to codebase and system configurations but no direct access to PII unless necessary for system debugging and maintenance.
c) Contractor Data Analyst: Read-only access to aggregated data sets. No access to individual-level PII.
d) Contractor Auditor: Read-only access specifically designed for compliance checks.
e) Contractor System Admin: Similar to an internal Administrator but with limited scope, only able to administer the sections of the system they are responsible for.

Need for PII Access:
Access to PII for contractors is restricted and only granted when necessary for their roles, such as system debugging, data validation, and compliance auditing.

By implementing these controls and processes, we adhere to privacy control AR-3, ensuring that contractor involvement aligns with privacy requirements and regulations.

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.

General Training
All users, including contractors and employees, are required to complete VA's annual Privacy and Security Awareness Training. This training covers general topics such as the Privacy Act, HIPAA compliance, and the secure handling of PII and PHI. It also includes scenarios and quizzes to test users' understanding of privacy policies and practices.

Program-Specific Training
In addition to general training, users involved with this specific Remote Patient Monitoring technology solution undergo specialized training modules that address healthcare data's unique aspects and sensitivities. This training focuses on:

a) Data Classification: Identifying different types of data, including PII and PHI, and understanding the level of sensitivity associated with each.
b) Data Handling Procedures: Steps to securely handle, transmit, and dispose of data within the context of the program.
c) Access Control: Understanding the roles and permissions within the system and the importance of least privilege access.
d) Incident Reporting: Procedures to report any security or privacy incidents related to the system.

On-the-Job Training
Regular on-the-job training sessions are conducted to reinforce good practices and to update staff on any changes in policies or regulations. These sessions are often delivered through webinars, team meetings, and newsletters.

Refresher Courses

Refresher courses are mandatory every year or whenever there is a significant update to the system or relevant laws and policies. These courses ensure that all users remain informed and updated on privacy practices.

Assessment and Certification

Post-training assessments are administered to gauge the effectiveness of the training. Users must pass this assessment to gain or retain access to the system.

Documentation

Completion of all training modules is documented, and records are maintained to ensure compliance with ongoing training requirements.

By implementing this multi-faceted training approach, we adhere to privacy control AR-5, ensuring that all individuals with access to PII are fully trained and aware of their responsibilities to protect this sensitive information.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* No
2. *The System Security Plan Status Date:* No
3. *The Authorization Status:* No
4. *The Authorization Date:* No
5. *The Authorization Termination Date:* No
6. *The Risk Review Completion Date:* No
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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.***

Target date: March 1, 2024

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)*

The RPM/HTH-D system is hosted in the VA Enterprise Cloud (VAEC) Amazon Web Services Government Cloud. The VAEC implements the NIST-, FedRAMP- and VA-required security controls for each system to obtain a VA Authority to Operate (ATO). The VAEC has met the FedRAMP High Authorization.

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.*

NA

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.

NA

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.

NA

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).

NA

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2023.10.25 11:16:40 -04'00'

Privacy Officer, Dennis Lahl

OLIVER PATAGUE Digitally signed by OLIVER PATAGUE
Date: 2023.10.24 06:33:27 -07'00'

Information System Security Officer, Oliver R. Patague

ELLEN HANS (Affiliate) Digitally signed by ELLEN HANS (Affiliate)
Date: 2023.10.24 14:30:48 -04'00'

Information System Owner, Ellen A. 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).

- **System of Records Notice (SORN)** (https://www.oprm.va.gov/privacy/systems_of_records.aspx)
  - *24VA10VA7/85 FR 62406 Patient Medial Records.* (24VA10A7/85 FR 62406)

- **VHA Handbook 1605.4, *Notice of Privacy Practices*, October 7, 2015** (1605_04_HK_2015-10-07.pdf)

- **Remote Patient Monitoring – Home Telehealth Enrollment Agreement Staff Guidance.** (Screenshots below)

Remote Patient Monitoring-
Home Telehealth Enrollment
Agreement Staff Guidance

July 2022

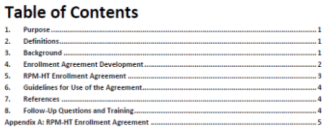
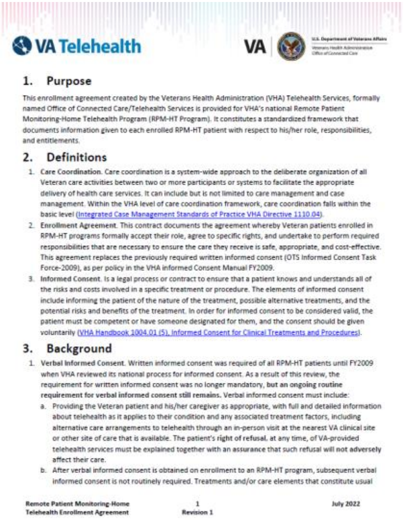


Table of Contents

-

Remote Patient Monitoring-Home Telehealth Enrollment Agreement i Revision 1 July 2022



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

1. Purpose

This enrollment agreement created by the Veterans Health Administration (VHA) Telehealth Services, formally named Office of Connected Care/Telehealth Services is provided for VHA's national Remote Patient Monitoring-Home Telehealth Program (RPM-HT Program). It constitutes a standardized framework that documents information given to each enrolled RPM-HT patient with respect to his/her role, responsibilities, and entitlements.

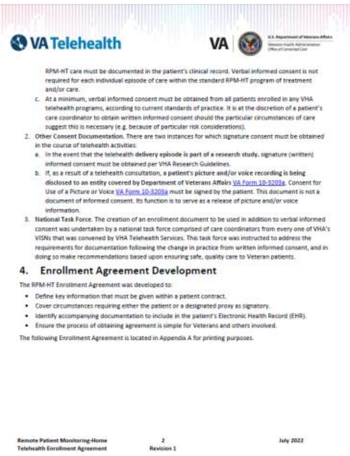
2. Definitions

1. **Care Coordination.** Care coordination is a system-wide approach to the deliberate organization of all Veteran care activities between two or more participants or systems to facilitate the appropriate delivery of health care services. It can include but is not limited to care management and case management. Within the VHA level of care coordination framework, care coordination falls within the basic level (Integrated Case Management Standards of Practice VHA Directive 1110.04).
2. **Enrollment Agreement.** This contract documents the agreement whereby Veteran patients enrolled in RPM-HT programs formally accept their role, agree to specific rights, and undertake to perform required responsibilities that are necessary to ensure the care they receive is safe, appropriate, and cost-effective. This agreement replaces the previously required written informed consent (OTS Informed Consent Task Force-2009), as per policy in the VHA informed Consent Manual FY2009.
3. **Informed Consent.** Is a legal process or contract to ensure that a patient knows and understands all of the risks and costs involved in a specific treatment or procedure. The elements of informed consent include informing the patient of the nature of the treatment, possible alternative treatments, and the potential risks and benefits of the treatment. In order for informed consent to be considered valid, the patient must be competent or have someone designated for them, and the consent should be given voluntarily (VHA Handbook 1004.01 (5), Informed Consent for Clinical Treatments and Procedures).

3. Background

1. **Verbal Informed Consent.** Written informed consent was required of all RPM-HT patients until FY2009 when VHA reviewed its national process for informed consent. As a result of this review, the requirement for written informed consent was no longer mandatory, **but an ongoing routine requirement for verbal informed consent still remains.** Verbal informed consent must include:
   a. Providing the Veteran patient and his/her caregiver as appropriate, with full and detailed information about telehealth as it applies to their condition and any associated treatment factors, including alternative care arrangements to telehealth through an in-person visit at the nearest VA clinical site or other site of care that is available. The patient's **right of refusal**, at any time, of VA-provided telehealth services must be explained together with an assurance that such refusal will not adversely affect their care.
   b. After verbal informed consent is obtained on enrollment to an RPM-HT program, subsequent verbal informed consent is not routinely required. Treatments and/or care elements that constitute usual

Remote Patient Monitoring-Home Telehealth Enrollment Agreement 1 Revision 1 July 2022



RPM-HT care must be documented in the patient's clinical record. Verbal informed consent is not required for each individual episode of care within the standard RPM-HT program of treatment and/or care.

c. At a minimum, verbal informed consent must be obtained from all patients enrolled in any VHA telehealth programs, according to current standards of practice. It is at the discretion of a patient's care coordinator to obtain written informed consent should the particular circumstances of care suggest this is necessary (e.g. because of particular risk considerations).

2. **Other Consent Documentation**. There are two instances for which signature consent must be obtained in the course of telehealth activities:
   a. In the event that the telehealth **delivery episode is part of a research study**, signature (written) informed consent must be obtained per VHA Research Guidelines.
   b. If, as a result of a telehealth consultation, **a patient's picture and/or voice recording is being disclosed to an entity covered by Department of Veterans Affairs** VA Form 10-3203a. Consent for Use of a Picture or Voice VA Form 10-3203a must be signed by the patient. This document is not a document of informed consent. Its function is to serve as a release of picture and/or voice information.
3. **National Task Force**. The creation of an enrollment document to be used in addition to verbal informed consent was undertaken by a national task force comprised of care coordinators from every one of VHA's VISNs that was convened by VHA Telehealth Services. This task force was instructed to address the requirements for documentation following the change in practice from written informed consent, and in doing so make recommendations based upon ensuring safe, quality care to Veteran patients.

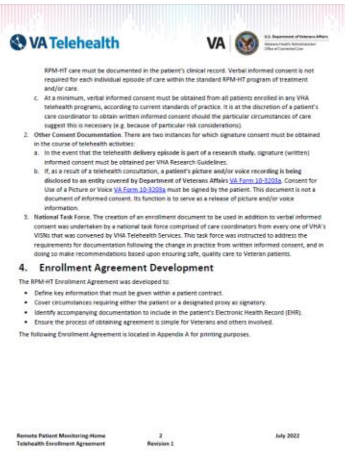
4. Enrollment Agreement Development

The RPM-HT Enrollment Agreement was developed to:

- Define key information that must be given within a patient contract.
- Cover circumstances requiring either the patient or a designated proxy as signatory.
- Identify accompanying documentation to include in the patient's Electronic Health Record (EHR).
- Ensure the process of obtaining agreement is simple for Veterans and others involved.

The following Enrollment Agreement is located in Appendix A for printing purposes.

Remote Patient Monitoring-Home Telehealth Enrollment Agreement 2 Revision 1 July 2022



RPM-HT care must be documented in the patient's clinical record. Verbal informed consent is not required for each individual episode of care within the standard RPM-HT program of treatment and/or care.

c. At a minimum, verbal informed consent must be obtained from all patients enrolled in any VHA telehealth programs, according to current standards of practice. It is at the discretion of a patient's care coordinator to obtain written informed consent should the particular circumstances of care suggest this is necessary (e.g. because of particular risk considerations).

2. **Other Consent Documentation**. There are two instances for which signature consent must be obtained in the course of telehealth activities:
   a. In the event that the telehealth **delivery episode is part of a research study**, signature (written) informed consent must be obtained per VHA Research Guidelines.
   b. If, as a result of a telehealth consultation, **a patient's picture and/or voice recording is being disclosed to an entity covered by Department of Veterans Affairs** VA Form 10-3203a. Consent for Use of a Picture or Voice VA Form 10-3203a must be signed by the patient. This document is not a document of informed consent. Its function is to serve as a release of picture and/or voice information.
3. **National Task Force**. The creation of an enrollment document to be used in addition to verbal informed consent was undertaken by a national task force comprised of care coordinators from every one of VHA's VISNs that was convened by VHA Telehealth Services. This task force was instructed to address the requirements for documentation following the change in practice from written informed consent, and in doing so make recommendations based upon ensuring safe, quality care to Veteran patients.

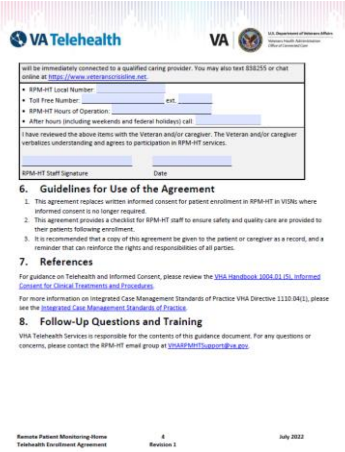
4. Enrollment Agreement Development

The RPM-HT Enrollment Agreement was developed to:

- Define key information that must be given within a patient contract.
- Cover circumstances requiring either the patient or a designated proxy as signatory.
- Identify accompanying documentation to include in the patient's Electronic Health Record (EHR).
- Ensure the process of obtaining agreement is simple for Veterans and others involved.

The following Enrollment Agreement is located in Appendix A for printing purposes.

Remote Patient Monitoring-Home Telehealth Enrollment Agreement 2 Revision 1 July 2022



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.

7. References

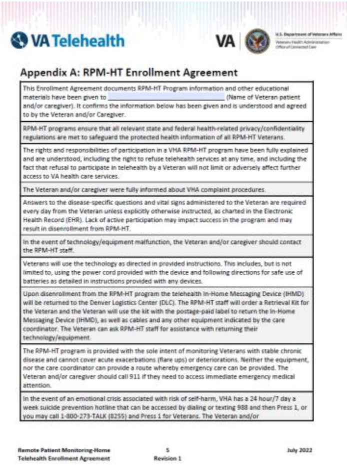
For guidance on Telehealth and Informed Consent, please review the VHA Handbook 1004.01 (5), Informed Consent for Clinical Treatments and Procedures.

For more information on Integrated Case Management Standards of Practice VHA Directive 1110.04(1), please see the Integrated Case Management Standards of Practice.

8. Follow-Up Questions and Training

VHA Telehealth Services is responsible for the contents of this guidance document. For any questions or concerns, please contact the RPM-HT email group at VHARPMHTSupport@va.gov.

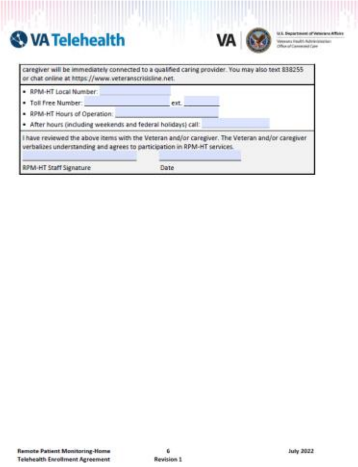
Remote Patient Monitoring-Home Telehealth Enrollment Agreement 4 Revision 1 July 2022



Appendix A: 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

Remote Patient Monitoring-Home Telehealth Enrollment Agreement 5 Revision 1 July 2022



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

Remote Patient Monitoring-Home Telehealth Enrollment Agreement 6 Revision 1 July 2022

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