Privacy Impact Assessment for the VA IT System called:

Remote Patient Monitoring /Home Telehealth – Cognosante

Veterans Health Administration

Office of Connected Care / Telehealth & Scheduling

eMASS ID # 2457

Date PIA submitted for review:

28-MAR-2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.Katz-Johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Stuart Chase	Stuart.Chase@va.gov	410-340-2018
Information System Owner	Ellen Hans	Ellen.Hans@va.gov	703-534-0205

Abstract

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

The Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) is the clinical desktop (system) hosted within the VAEC (VA Enterprise Cloud). Patients manually input health data, medications, biometric information, and respond to Disease Management Protocols (DMP). The Mobile Application will transmit de-identified Protected Health Information (PHI) and Personally Identifiable Information (PII) from the device to the server.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 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 – Cognosante (RPM/HT-C) is the clinical desktop (system) hosted within the VAEC (VA Enterprise Cloud). The system is only accessible from within the VA boundary and can only be accessed by authorized and authenticated VA Care Coordinators. This remote patient monitoring / home telehealth (RPM / HT) system of Home Telehealth – Cognosante has several different platforms; CareConsole Hub (Mobile App Cellular), CareConsole Video Hub (Mobile Video App Cellular), CareConsole Mobile Application (Downloadable App), CareConsole Web (Web Enabled), CareConsole Web with Modem (Web + Gateway), CareConsole Interactive Voice Response (IVR) and CareConsole Voice with Modem (IVR + Gateway). Patients manually input Health Data, Medications / biometric information and respond to Disease Management Protocols (DMP) presented directly on the web page or respond verbally via IVR. Patients utilizing the CareConsole Hub, Video Hub, Modem, or Mobile Application will connect directly to the servers via an approved Virtual Private Network /Internet Protocol Security (VPN/IPSEC) tunnel. CareConsole Hub, Video Hub, Modem, and Mobile Application will transmit de-identified Protected Health Information (PHI) and Personally Identifiable Information (PII) from the device to the server. The VAEC host all servers and appliances related to the Cognosante platform offerings.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

This is a VA owned and non-VA operated system. It is administered by the Veterans Heath Administration Office of Connected Care / Telehealth & Scheduling.

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

The number of individuals is determined by the enrollment of Veteran patients by VA Care Coordinators. At this time, we have ~20K active patients and ~60K inactive (past) patients. We would anticipate a continual increase in active patients as the contract continues. Individuals referred to the Home Telehealth program require daily vitals monitoring that can be done on their own from the comfort of their homes.

Check if Applicable	Demographic of Individuals
☒	Veterans or Dependents
☐	VA Employees
☐	Clinical Trainees
☐	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

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

The Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) system is an information system which is being utilized for the collection, processing, maintenance, use, sharing, dissemination, and disposition of VA Sensitive Information/Data which includes:

- Individually Identifiable Information (III),
- Individually Identifiable Health Information (IIHI),
- Information in the Identifiable Form (IIF),
- Personally Identifiable Information (PII),
- Protected Health Information (PHI), and
- Sensitive Personal Information (SPI).

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

Internal Sharing:

Depending on your clinical requirement, periodic adjustments to the patient information may need to flow back and forth between VistA and Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) system.

1. Home Telehealth Reporting (HTR): PII/PHI

2. Veterans Health Administration (VHA): IT System Name: Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C): PII, PHI and Individually Identifiable Information (III)

3. VA VistA: Information commonly updated during a patient's enrolled state are medication, address and contact information. PII, PHI and Individually Identifiable Information (III)

4. HDR: PII/PHI

5. MPI: PII/PHI

External Sharing:

1. The Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) System Hub, a home medical device, is located at the VA patient home (an external organization).

2. Remote Patient Monitoring / Home Telehealth – Cognosante – CareConsole Video Hub - Mobile Video App Cellular (VA Patient)

3. Remote Patient Monitoring / Home Telehealth – Cognosante – CareConsole Mobile Application - Downloadable App (VA Patient)

4. Remote Patient Monitoring / Home Telehealth – Cognosante - Web – Web Enabled (VA Patient)

5. Remote Patient Monitoring / Home Telehealth – Cognosante - CareConsole Web with Modem – Web + Gateway (VA Patient)

6. Remote Patient Monitoring / Home Telehealth – Cognosante – CareConsole Interactive Voice Response (IVR) (VA Patient)

7. Remote Patient Monitoring / Home Telehealth – Cognosante - CareConsole Voice with Modem - IVR + Gateway (VA Patient)

8. Veteran Health Administration (VHA) - Unified Electronic Health Record (EHR) (DOD Defense Health Agency – Cerner)

F. Are the modules/subsystems only applicable if information is shared?

Yes

G. Is the system operated in more than one site to include primary and secondary 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?

No, the Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) is the clinical desktop (system) hosted within the VA VAEC (VA Enterprise Cloud). The system is only accessible from within the VA boundary and can only be accessed by authorized and authenticated VA Care Coordinators.

3. Legal Authority and System of Record Notices (SORN)

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

I. What is the SORN?

SORN 24VA10A7 / 85 FR 62406, *Patient Medical Records-VA* (10/2/2020)
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

SORN 173VA005OP2 / 86 FR 61852, *VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC-MAP)* (11/8/2021)
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf

J. SORN revisions/modification

The SORN does not require revisions nor modifications.

K. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

No, the SORN will not require amendment or revision and approval.

4. System Changes

L. Will the business processes change due to the information collection and sharing?

☐ Yes
☒ No

M. *Will the technology changes impact information collection and sharing?*

☐ Yes
☒ No

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 Information 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
☒ **Full** Social Security Number
☒ **Partial** 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
☒ Sex
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Date of Death
☐ Business Email Address
☒ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (List Below)

Other PII/PHI data elements: Administrative Sex, Biometric Information, Device Serial Number, Health Data, Medicaid ID, Password, Patient Nickname, Personal Identification Number (PIN), Primary Language, User Name.

1.2 List 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?

This information is collected from both the Veteran patient and via connections between the VA Vista/VA Cerner Electronic Health Record and the RPM/HT-C information system. Data can also be updated via Veteran communication with the VA Care Coordinator and RPM/HT-C.

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.

Data is collected from sources listed in section 1.2a (above) other than the individual in order to maintain the integrity of the data as well as support traceability.

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

CareConsole is the source of information which allows for the creation of reports of patient data.

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

1.3 Methods of information collection

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Information collected from Individuals: The two most critical stakeholders for Care Coordination are the Veteran and the Clinician. Mobile device platform and mobile applications are used to collect objective and subjective health information from the Veteran, deliver the data to the clinician who provides care, and eventually transfer some data to VistA.

Information collected from Technology: Patients use devices and applications to collect information via a web browser, mobile application, telephone, vitals devices, and peripherals. The following devices are used in the collection of information; Product Interoperability lists the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System a la carte data collection via Hub, Interactive Voice Response (IVR), mobile device platform, mobile applications, and interoperable peripherals/accessories currently in use by Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) System customers.

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?

Information is not collected on a form. All information is recorded in CareConsole using HL7 integration between VistA/Cerner and the Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) information system (CareConsole).

1.4 Information checks for accuracy, and 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 Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) System allows the clinicians and patient to manage/monitor the information included in the patient's profile. The Veterans' identifying information is checked for accuracy by the Clinicians and is cross-referenced with information via Veterans coordinators.

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?

The Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) information system does not use a commercial aggregator.

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. It operates under the legal authority of Title 38, United States Code, Sections 501(b) and 304.

The VA Home Telehealth Contract # C03 36C79123D0002 issued to Cognosante on 6/1/2023 authorizes Cognosante to collect and process the information related to VA home telehealth patients. The data is provided by VA.

It operates under the legal authority of Title 38, United States Code, Sections 501(b) and 304 and collects information under the System of Record of VA SORN 24VA10A7 / 85 FR 62406 – Patient Medical Records –VA and SORN 173VA005OP2 / 86 FR 61852 – VA Enterprise Cloud – Mobile Application Platform (Cloud)

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

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

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

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

<u>Principle of Minimization:</u> The information is directly relevant and necessary to accomplish the specific purposes of the program.

<u>Principle of Individual Participation:</u> The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: *VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*
This 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: VA patients and clinicians will be able to capture and upload PII/SPI through approved mobile devices. Use of mobile devices (i.e., smartphones and tablets) present potential privacy risks because of the inherent portability of the devices thus making them especially vulnerable to loss and theft.
The system collects, processes, and retains PII and PHI on Veterans. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.

Mitigation: In order to mitigate the privacy risks associated with the use of mobile devices, Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) system has developed a mobile application for Mobile Device. The Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) system CareConsole Mobile application incorporates the latest in mobile smartphone and tablet technology on the Android and Apple operating system platforms. Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) System uses the latest in secure communication such as secure web pages and private key encryption.

Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 (or successor) encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	The patient's first name and the last name is collected as part of the new patient register process within the Remote Patient Monitoring / Home	The patient's first name and the last name is collected as part of the new patient register process within the Remote Patient Monitoring / Home

PII/PHI Data Element	Internal Use	External Use
	Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement for patients to answer this Data Element for registration. Additionally, The Care Coordinator is able to view additional details about a patient by clicking on a patient's name.	Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement for patients to answer this Data Element for registration. Additionally, The Care Coordinator is able to view additional details about a patient by clicking on a patient's name.
Full Social Security Number	The patient's SSN is collected as part of the new patient registration process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement for patients to answer this data element for registration.	The patient's SSN is collected as part of the new patient registrations process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement for patients to answer this data element for registration.
Partial Social Security Number	The patient's partial SSN is used as a primary identifier within the CareConsole Application.	Not Used
Date of Birth (DoB)	The patient's DoB is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement for patients to answer this data element for registration.	The patient's DoB is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement for patients to answer this data element for registration.
Mother's Maiden Name	The patient's Mother's Maiden Name is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement for patients to answer this data element for registration.	Not used
Personal Mailing Address	The patient's Mailing Address is collected as part of the new patient register process within	Not used

PII/PHI Data Element	Internal Use	External Use
	the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal. The patient's Zip Code is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal.	
Personal Phone Number(s)	The patient's phone number is collected as part of the Interactive Voice Response (IVR) passcode requirement process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal.	The patient's phone number is collected as part of the Interactive Voice Response (IVR) passcode requirement process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal.
Personal Email Address	The patient's email address is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement for patients to answer this data element for registration.	The patient's email address is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement for patients to answer this data element for registration.
Emergency Contact Information	The patient's emergency contact information is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement for patients to answer this data element for registration.	Not used
Medications	The patient's Medications are collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement	Not used

PII/PHI Data Element	Internal Use	External Use
	for patients to answer this data element for registration.	
Sex	The patient's sex is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement for patients to answer this data element for registration.	Not used
Administrative Sex	The patient's Administrative Sex is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement for patients to answer this data element for registration.	Not used
Biometric Information	The patient’s biometrics information is collected in order to provide health care providers with a status of the patient’s health. Vitals information will vary based on the health condition being monitored.	The patient’s biometrics information is collected in order to provide health care providers with a status of the patient’s health. Vitals information will vary based on the health condition being monitored.
Device Serial Numbers	The device serial number is collected to link device assignment to specific patients.	Not used
Electronic Data Interchange Personal Identifier (EDIPI)	The EDIPI is a unique member identifier that allows the VA to retrieve the Veteran’s health record.	The EDIPI is a unique member identifier that allows the VA to retrieve the Veteran’s health record.
Health Data	The patient’s subjective health information (e.g. medications, diet, pain, mood) is collected in order to provide health care providers with a status of the patient’s health. The type of information varies based on the health condition being monitored.	The patient’s subjective health information (e.g. medications, diet, pain, mood) is collected in order to provide health care providers with a status of the patient’s health. The type of information varies based on the health condition being monitored.

PII/PHI Data Element	Internal Use	External Use
Integration Control Number (ICN)	The platform allows for the use of ICN for recording, storing, or retrieving patient information. The ICN is another patient unique identifier which can be used to search and retrieve patient information.	The platform allows for the use of ICN for recording, storing, or retrieving patient information. The ICN is another patient unique identifier which can be used to search and retrieve patient information.
Medicaid ID	The patient's Medicaid ID is collected as a secondary identifier for the patient.	Not used
Password	The patient's password is created and collected to allow for server side application authentication of the patient.	The patient's password is created and collected to allow for server side application authentication of the patient.
Patient Nickname	Not used	The patient's Nickname is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System portal. This information is a requirement for patients to answer this data element for registration.
Personal Identification Number (PIN)	The patient's PIN is created and collected to allow for device side application authentication of the patient.	The patient's PIN is created and collected to allow for device side application authentication of the patient.
Primary Language	The patient's primary language is collected to provide service in the language the patient is most comfortable using, as their primary language.	Not used
User Name	The patient's user name is created and collected to allow for server side application authentication of the patient.	The patient's user name is created and collected to allow for server side application authentication of the patient.

2.2 Describe the types of tools 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?

Information received and maintained by the portal is subjective health information gathered by medical devices located in the Veterans' homes. The medical devices used in the Veterans' home vary based on the type of medical condition being monitored. The sources of information are a combination of devices and tools which patients use to answer symptomatic questions and generate data readings to complete a health check (or status of health). This could include blood pressure, weight, and other vitals data.

As the device and or tools read and record the patient data, the data is transmitted into the Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) System so the data can be viewed within the portal by clinicians. Collection of this data is required to assist clinicians in providing care for their patients in an efficient and effective manner. The portal is a source of information as it generates a value (and in some cases an alert) based on the parameters set by clinicians.

The Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) System develops the following reports:

• Enrolled/Active Report
• Patient Report for an IVR Survey
• Patient Status Report
• New Patient Referral Report
• Priority Alert Readings
• Non-Responder Reports

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.

As the device and or tools read and record patient data, the data is transmitted into the Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) information system so the data can be viewed within the portal by VA Care Coordinators. The readings and responses collected are added to the individual's existing patient record maintained within the information system's database. Collection of this data is required to assist VA Care Coordinators in providing care for their patients in an efficient, safe, and effective manner. The portal is a source of information as it generates a value (and in some cases an alert) based on the parameters set by clinicians.

By interpreting this newly derived information, decisions on the direction of treatment and management of the patient's morbidity will be taken by the supporting VA Care Coordinator.

2.3 How the information in the system is 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?

All servers and appliances will be configured to best practices prior to provisioning within VAEC, and Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) System will configure according to the latest hardening guides. Additionally, all servers and appliances will be scanned for vulnerabilities and patched to ensure any deficiencies are addressed prior to installation at the VA data center. A system security plan will be maintained and shared as needed with the primary VA POC to ensure we meet the Authorization to Operate (ATO). Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) System servers have been designed for both expandability and redundancy to ensure system uptime in compliance with the requirements and will meet the needs of the contract. Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) System servers will be equipped with a remote access controller that will allow us to power on/off and access the servers during maintenance.

The Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) System is hosted within the VA Enterprise Cloud (VAEC). The Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) system is only accessible from within the VA perimeter and will only be accessed by Care Coordinators. The Web-Enabled content is accessible from the public Internet and is accessible to patients enrolled in the VA Home Telehealth program. The VAEC will host all servers and appliances related to the Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) system. The following services will be supported by our servers: Web services, database, Health Layer 7 (HL7) integration, Remote Access Server (RAS), IVR, and Internal Test Lab (ITL).

A Site-to-Site Virtual Private Network (VPN) gateway will be hosted at our VAEC instance and it will be used to support cellular connectivity from patient monitoring devices. The portal will be designed with redundancy across hardware and virtualization to ensure optimal uptime is achieved (where applicable).

Transport layered security and secure web pages are employed to protect data in transit and full volume encryption on the servers is used to protect data at rest.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) System leverages the latest in secure communication and encryption standards such as HTTPS over SSL/TLS, utilizing AES 256 for private key encryption, RSA-2048 for public key encryption, and SHA-256 for key hashing. For protection of sensitive information such

as SSN, depending on the page a client is on, it may display partial SSN (i.e. last 4) with the option to hover over the SSN to display the full SSN.

Additional protections such as firewalls, network segmentation, Access Control List (ACL), Virtual Private Network (VPN), and Multi-Factor Authentication (MFA) are employed to further protect SSNs.

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

PII/PHI is safeguarded in accordance with OMB Memorandum M-06-15 through the use of administrative controls such VA Rules of Behavior (ROB) and VA annual training in addition to the technical controls mentioned above.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

The Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) system is maintained by Cognosante. Cognosante is contracted by the Department of Veterans Affairs (VA) Denver Logistics Center's (DLC's) Home Telehealth (HT) Initiative to provide support and assistance to the program. The VA Cognosante contract is reviewed annually by both the Cognosante team and VA Contract Officer's Representative (COR) to ensure compliance with the performance work statement.
Cognosante staff will have appropriate authorized access to the portal as part of assigned development, maintenance, and troubleshooting duties. Cognosante personnel involved in the operations of the Home Telehealth system complete the VA Security Clearance process.

The following documents are reviewed signed annually by each team member:
- Cognosante Employee Handbook Acknowledgement Form
- Cognosante Non-Disclosure Agreement
- VA Contractor Rules of Behavior

With regard to VA Care Coordinator access to PII, specifically for initial site setup, HTH-Cognosante provides a form the VA Site Lead fills out to create the VA site and provides a list of VA Site Admin users for the site. The form includes details such as station ID and DUZ information for VistA integration. HTH-Cognosante then creates the site and the requested VA Site Admin Users. Once the VA site is created and the VA admin users are set up, the VA admin users are able to create and manage new VA non-admin users. HTH-Cognosante will also create new users at the direct request of the VA Site Lead.

With regard to veterans (patients) access to PII, veterans are selected for the remote patient monitoring telehealth program and assigned devices (e.g. hub/tablet, peripherals (blood pressure monitor, weight scale, etc)) as part of the onboarding process conducted by the VA Care Coordinator. Veterans who participate in the remote patient monitoring telehealth program have access to only their own PII/PHI.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Yes, the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) _AC_SOP-FINAL (Please note: AC is Access Control and SOP is Standard Operarating Procedure) which references the organization-level policy that outlines the policies and procedures regarding the correct use and management of access controls to the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) system. Access controls shall be implemented on all Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) information systems, to include VA assigned devices with approved access to Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System information to protect against loss of confidentiality, integrity, or availability.

2.4c Does access require manager approval?

Yes, only those VA Care Coordinators who have a PIV card (which has been approved by the manager and VA COR) as well as Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) CareConsole credentials will be granted access.

Yes, veterans (patients) are selected for the remote patient monitoring telehealth program and assigned devices (e.g. hub/tablet, peripherals (blood pressure monitor, weight scale, etc)) as part of the onboarding process conducted by the VA Care Coordinator.

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

Yes, access to all Protected Health Information (PHI/PII) is monitored, tracked, and recoded by the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) information system and audit records are stored and maintained within the application database.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

This is a shared responsibility between RPM/HT-C and VA; for administrative safeguards related to the protection of PHI/PII, the RPM/HT-C System Steward, VA Information System Owner, and VA Information System Security Office would be responsible.

For Technical safeguards related to the protection of PHI/PII, the vendor, RPM/HT-C, would be responsible.

In the event of a breach, the procedure detailed within the RPM/HT-C Incident Response Plan (IRP) would be enabled. The IRP is reviewed and updated (as necessary) annually or when a major change to the process is made. The table top exercise of the IRP is conducted annually.

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*

- Name
- Full Social Security Number
- Partial Social Security Number
- Date of Birth
- Mother's Maiden Name
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Email Address
- Emergency Contact Information
- Medications
- Sex
- Administrative Sex
- Biometric Information
- Device Serial Number
- EDIPI (Electronic Data Interchange Personal Identifier)

- Health Data
- Integrated Control Number (ICN)
- Medicaid ID
- Password
- Patient Nickname
- Personal Identification Number (PIN)
- Primary Language
- User Name

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

In compliance with VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP) (173VA005OP2): Records from this system that are needed for audit purposes will be disposed of 6 years after a user's account becomes inactive. Routine records will be disposed of when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes. These retention and disposal statements are pursuant to NARA General Records Schedules GRS 20, item 1c and GRS 24, item 6a.

In compliance with Patient Medical Records-VA (24VA10A7): 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, 6000.1d (N1-15-91-6, Item 1d) and 6000.2b (N1-15-02-3, Item 3).

3.3 The retention schedule 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. Please work with the system VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

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

Yes, the Records Control Schedule (RCS) 10-1 provides VHA records retention and disposition requirements for VHA Central Office, Program Offices, and field facilities. The VHA Records Control Schedule (RCS) 10-1 is the main authority for the retention and disposition requirements of VHA records. It provides a brief description of the records and states the retention period and disposition requirements. VHA RCS 10-1, dated January 2019 is found at this link: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf.

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

VA SORN - Policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records.

VA Patient Medical Record Retention & Disposal: 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 75 years after the last episode of patient care then destroyed/deleted.

VHA RCS 10-1 Section 1006.13. Personally identifiable information extracts. System-generated or hardcopy printouts generated for business purposes that contain Personally Identifiable Information. Temporary; destroy when 90 days old or no longer needed pursuant to a supervisory authorization, whichever is appropriate.

VHA RCS 10-1Section 1006.14. Personally identifiable information extract logs. Logs that track the use of PII extracts by authorized users, containing some or all of: date and time of extract, name and component of information system from which data is extracted, user extracting data, data elements involved, business purpose for which the data will be used, length of time extracted information will be used. Also includes (if appropriate): justification and supervisory authorization for retaining extract longer than 90 days and anticipated disposition date. Temporary: destroy when business use ceases. (GRS 4.2 item 140, DAA-GRS-2013-0007-0013)

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.

As the Covered Entity, customer data is owned by VA; therefore, RPM/HT-C, as the Business Associate acting on behalf of the Covered entity, retains the data indefinitely and does not destroy any data (subject to terms and conditions of the executed Business Associate Agreement (BAA) and/or PWS).

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.

This system does not use PII for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) 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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

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

Follow the format below:

Privacy Risk: There is a potential privacy risk that records within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System due to the length of retention which is indefinite (refer to section 3.4).

Mitigation: To mitigate this risk, Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System implements administrative and technical safeguards to protect this information such as role based authentication to support separation of duties and least privilege to encryption of data at rest, encrypted backups, and deidentification of data outside of VA perimeter where it is only re-identified and associated with the specific patient record upon upload to the information system's servers behind VA perimeter.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) consists of 10 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 – Cognosante (RPM/HT-C) 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 3.9a 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**
Home Telehealth Reporting (HTR)	Yes	Yes	• Name • Full Social Security Number • Date of Birth • ICN (Integrated Control Number) • EDIPI	This is an important HW component for meeting the VA HL7 integration requirements. PII is sent to us by the Census integration engine, and PHI is sent back from the Care Console	All HL7 message traffic performed behind VAEC firewall.

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
				system to ensure seamless integration with Census, and the Care Console always has latest patient correct information	
CareConsole Database	Yes	Yes	• Name • Full Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Emergency Contact Information • Sex • Primary Language • Personal Email Address • Health Data • Medications	HTH Monitoring and Alerting	Behind va.gov firewall. All data transmitted is encrypted in transit and encrypted while at rest.

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
			• Biometric Information		
CareConsole Application	Yes	Yes	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Emergency Contact Information • Sex • Primary Language • Personal Email Address • Health Data • Medications • Biometric Information	HTH Monitoring and Alerting	All data transmitted is encrypted in transit and encrypted while at rest.

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
Veterans Health Administration (VHA) VistA Systems / IT System Name: VistA	Yes	Yes	• Name • Full Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Emergency Contact Information • Sex • Primary Language • Personal Email Address • Health Data • Medications • Biometric Information	This is an important HW component for meeting the VA HL7 integration requirements. PII is sent to us by the VA VistA integration engine, and PHI is sent back from the Care Console system to ensure seamless integration with VistA, and the Care Console always has latest patient correct information	All HL7 message traffic performed behind VAEC firewall.
MPI (Master Patient Index)	Yes	Yes	• Name • Mother's Maiden Name • Full Social Security	This is an important HW component for meeting	All HL7 message traffic performed behind

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
			Number • Date of Birth • ICN (Integrated Control Number) • Administrative Sex • Personal Mailing Address • Personal Phone Number(s)	the VA HL7 integration requirements. PII is sent to us by the MPI integration engine, and PHI is sent back from the Care Console system to ensure seamless integration with MPI, and the Care Console always has latest patient correct information	VAEC firewall.
HDR (Health Data Repository)	Yes	Yes	• Name • Full Social Security Number • Date of Birth • ICN (Integrated Control Number) • Biometric Information	This is an important HW component for meeting the VA HL7 integration requirements. PII is sent to us by the HDR integration	All HL7 message traffic performed behind VAEC firewall.

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
				engine, and PHI is sent back from the Care Console system to ensure seamless integration with HDR, and the Care Console always has latest patient correct information	

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Home Telehealth Reporting (HTR)	This is an important HW nomponent for meeting the VA HL7 integration requirements. PII is sent to us by the Census integration engine, and PHI is sent back from the Care Console system to ensure seamless integration with Census, and the Care Console always has latest patient correct information	• Name • Social Security Number • Date of Birth • ICN (Integrated Control Number) • EDIPI	HL7 point-to-point LowerLevel Protocol (LLP) to Census from Cognosante
Veterans Health Administration (VHA)	HTH Monitoring and Alerting	• Name • Social Security Number • Date of Birth	Data is transmitted from the patient sensors to the

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
IT System Name: Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C)		• Personal Mailing Address • Personal Phone Number(s) • Emergency Contact Information • Sex • Primary Language • Personal Email Address • Health Data • Medications • Biometric Information	medical device via Bluetooth. The medical device transfers the data to the servers through cellular / VA IPSec tunnel, analog modem via Plain Old Telephone System (POTS), or WIFI. Patients may also interact with IVR (Interactive Voice Recognition) software package
Veterans Health Administration (VHA) VistA Systems / IT System Name: VistA	This is an important HW component for meeting the VA HL7 integration requirements. PII is sent to us by the VA VistA integration engine, and PHI is sent back from the Care Console system to ensure seamless integration with VistA, and the Care Console always has latest patient correct information	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Emergency Contact Information • Sex • Primary Language • Personal Email Address • Health Data • Medications • Biometric Information	The integration approach is a Patient Visit Update (ADT (Admissions, Discharges, Transfers)-A08) message in either direction.
Veterans Health Administration	This is an important HW component for meeting the VA HL7	• ICN (Integrated Control Number)	HL7 point-to-point Lower Level Protocol

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
Health Data Repository (HDR)	integration requirements. PII is sent to us by the HDR integration engine, and PHI is sent back from the Care Console system to ensure seamless integration with HDR, and the Care Console always has latest patient correct information	• Biometric Information	(LLP) to HDR from Cognosante
Veterans Health Administration Master Patient Index (MPI)	This is an important HW component for meeting the VA HL7 integration requirements. PII is sent to us by the HDR integration engine, and PHI is sent back from the Care Console system to ensure seamless integration with HDR, and the Care Console always has latest patient correct information	• Name • Mother's Maiden Name • Social Security Number • Date of Birth • ICN (Integrated Control Number) • Administrative Sex • Personal Mailing Address • Patient Phone	HL7 point-to-point Lower Level Protocol (LLP) bidirectional between MPI and Cognosante

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk: The privacy risk associated with sharing data within the Department of Veterans' Affairs is that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by VA personnel. All Home Telehealth users with access to the data received from Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) have a current Home Telehealth VA personnel clearance.

Home Telehealth – Cognosante will ensure that its employees take the annually required Privacy and HIPAA Training and VA Privacy and Information Security Awareness and Rules of Behavior Training provided through the Talent Management System (TMS) portal. The Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System is only accessible from within the VA and will only be accessed by VA Care Coordinators. The following services will be supported by our servers: Web services, database, Health Layer 7 (HL7) messaging, Remote Access Server (RAS), Integrated Voice Response (IVR) and Internal Test Lab (ITL). A Site to Site (S2S) VPN will be hosted at the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) VA Enterprise Cloud (VAEC) and will be used to support cellular/Wi-Fi connectivity from patient medical devices. The connections are controlled using physical access devices and/or guards. Individual users will not have access to the data except through the system security software inherent to the operating system. Access is controlled by authentication methods to validate the approved users. The FIPS 140-2 (or successor) certificate number of Home Telehealth – Cognosante' s gateway cryptographic module for establishing the VPN tunnel is FIPS 140-2 (or successor) certified. User Access control is managed by strong authentication method and must be assigned on the "Least Privilege" Principal. VA utilizes 2-factor authentications for general users. Elevated accounts must utilize a PIV card w/ PIN and authenticate to the server using a unique username and password. Technical security controls and services; designing security controls for customers; monitoring VA's secure Internet gateway, including secure web servers; ensuring antivirus protection across our network; ensuring critical operating system patches are installed; monitoring firewalls and router access control lists; monitoring private, dedicated high-speed communication links and site-to-site VPNs.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Remote Patient Monitoring / Home Telehealth -	The patient's biometrics information, Medications, Health Data,	CareConsole Hub is a home medical device which transmits: • Biometric Information	Pending new ISA/ MOU	Virtual Private Network /Internet

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
Cognosante (RPM/HT-C) CareConsole Hub Device - Mobile App Cellular (VA Patient)	and Patient Nickname are collected in order to provide health care providers with a status of the patient's health. Vitals information will vary based on the health condition being monitored. The patient's subjective health information is collected in order to provide health care providers with a status of the patient's health. The type of information varies based on the health condition being monitored.	• Medications • Health Data • Patient Nickname		Protocol Security (VPN/IPSEC) Plain Old Telephone System (POTS)

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
Remote Patient Monitoring / Home Telehealth – Cognosante – CareConsole Video Hub - Mobile Video App Cellular (VA Patient)	Patients manually input Health Data, Medications / biometric information and respond to Disease Management Protocols (DMP) presented directly on the hub or respond via video app.	CareConsole Video Hub is a home medical device which transmits: • Biometric Information • Medications • Health Data • Patient Nickname	Pending new ISA/ MOU	Virtual Private Network /Internet Protocol Security (VPN/IPSEC)
Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) CareConsole Web Enabled with Modem (VA Patient)	The patient's self-reported biometrics information, health data, medications, email address, username, and password are collected in order to provide health care providers with a status of the patient's health. Vitals information will vary	CareConsole Web Enabled is the web based patient accessible portal that transmits: • Biometric Information • Health Data • Medications • Personal Email Address • Username • Password	Pending new ESCCB ticket for external connection and new ISA/ MOU	Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) CareConsole Web Enabled with Modem (VA Patient)

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
	based on the health condition being monitored. The patient's subjective health information is collected in order to provide health care providers with a status of the patient's health. The type of information varies based on the health condition being monitored. The patient's email address is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth –			

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
	Cognosante (RPM/HT-C) system portal. This information is a requirement for patients to answer this data element for registration. The patient's user name is created and collected to allow for server side application authentication of the patient. The patient's password is created and collected to allow for server side application authentication of the patient.			
Remote Patient Monitoring / Home Telehealth – Cognosante - CareConsole Web with	The patient's self and/or device reported biometrics information, health data,	CareConsole Web Enabled is the web based patient accessible portal that transmits: • Biometric Information • Health Data	Pending new ISA/ MOU	HTTPS Web

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
Modem – Web + Gateway (VA Patient)	medications, email address, username, and password are collected in order to provide health care providers with a status of the patient's health. Vitals information will vary based on the health condition being monitored. The patient's subjective health information is collected in order to provide health care providers with a status of the patient's health. The type of information varies based on the health	• Medications • Personal Email Address • Username • Password		

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
	condition being monitored. The patient's first name and the last name is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) system portal. This information is a requirement for patients to answer this Data Element for registration. Additionally, The Care Coordinator is able to view additional details about a patient by clicking on a			

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
	patient's name.			
Remote Patient Monitoring / Home Telehealth – Cognosante – CareConsole Interactive Voice Response (IVR) (VA Patient)	The patient's self-reported biometrics Information, health data, name, personal phone number(s), and personal identification number (PIN) are collected in order to provide health care providers with a status of the patient's health. Vitals information will vary based on the health condition being monitored. The patient's subjective health information is collected in order to	CareConsole IVR is phone-based patient accessible portal that transmits: • Biometric Information • Health Data • Name • Personal Phone Number(s) • Personal Identification Number (PIN)	Care Coordinators assessment treatment plan note / VA Contract #C03 36C79123D000 2	Plain Old Telephone System (POTS)

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
	provide health care providers with a status of the patient's health. The type of information varies based on the health condition being monitored. The patient's first name and the last name are collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) system portal.			
Remote Patient Monitoring / Home	The patient's self-reported and/or	CareConsole IVR is the phone-based patient accessible portal that transmits:	Care Coordinators assessment treatment plan	Virtual Private Network /Internet

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
Telehealth – Cognosante - CareConsole Voice with Modem - IVR + Gateway (VA Patient)	device reported biometrics Information, health data, name, personal phone number(s), and personal identification number (PIN) are collected in order to provide health care providers with a status of the patient's health. Vitals information will vary based on the health condition being monitored. The patient's subjective health information is collected in order to	• Biometric Information • Health Data • Name • Personal Phone Number(s) • Personal Identification Number (PIN)	note / VA Contract #C03 36C79123D0002	Protocol Security (VPN/IPSEC)

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
	provide health care providers with a status of the patient's health. The type of information varies based on the health condition being monitored. The patient's first name and the last name are collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) system portal.			

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Veteran Health Administration (VHA) - Unified Electronic Health Record (EHR) (DOD Defense Health Agency – Cerner)	The patient's first name and the last name is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) system portal. This information is a requirement for patients to answer this Data Element for registration. Additionally, The Care Coordinator is able to view additional details about a patient by clicking on a	• Name • Full Social Security Number • Date of Birth • Integrated Control Number (ICN) • EDIPI (Electronic Data Interchange Personal Identifier) • Biometric Information • Medications	MEDCOI ISA – ID 733	IPSec tunnel utilizing Joint Security Architecture (JSA) across MedCOI (Medical Community of Interest)

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
	patient's name. The patient's SSN is collected as part of the new patient register process within the Remote Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) system portal. This information is a requirement for patients to answer this data element for registration. The patient's DoB is collected as part of the new patient register process within the Remote			

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
	Patient Monitoring / Home Telehealth – Cognosante (RPM/HT-C) system portal. This information is a requirement for patients to answer this data element for registration. The platform allows for the use of ICN for recording, storing, or retrieving patient information. The ICN is another patient unique identifier which can be used to search and retrieve patient information.			

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
	The EDIPI is a unique member identifier that allows the VA to retrieve the Veteran's health record. The patient's biometrics information, name, social security number, date of birth, integrated control number (ICN), EDIPI (Electronic Data Interchange Personal Identifier), and medications are collected in order to provide health care providers with a status of the patient's			

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
	health. Vitals information will vary based on the health condition being monitored. The patient's subjective health information is collected in order to provide health care providers with a status of the patient's health. The type of information varies based on the health condition being monitored.			

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: There is a risk that the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System data may be shared with unauthorized users or authorized users may share it with other unauthorized individuals. which may result in disclosure of protected information.

Mitigation: Outside organizations provide their own level of security controls such as access control, authentication and user logs to prevent unauthorized access. All personnel with access to Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System adheres to all information security requirements instituted by the VA Office of Information Technology (OIT). Information is shared in accordance with VA Handbook 6500

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

Verbal notice is provided to the individual before collection of the information as part of the onboarding/enrollment process conducted by the VA Care Coordinator.

Written notice is provided through the VHA Notice of Privacy Practice (NOPP) which explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter. https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

This Privacy Impact Assessment (PIA) also serves as notice. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." Notice is also provided in the Federal Register with the publication of the SORN.

Privacy Impact Assessment
https://department.va.gov/privacy/privacy-impact-assessments/

24VA10A7 / 85 FR 62406, Patient Medical Records-VA (10/2/2020)
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

SORN 173VA005OP2 / 86 FR 61852, VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC-MAP) (11/8/2021)
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf

6.1b If notice was not provided, explain why.

Notice was provided as indicated above.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

Notice is provided to the individual before collection of the information. Notice is provided via a system of records notice.The notice provided is adequate because it provides effective notice to individuals regarding the RPM/HT-C activities that impact privacy (including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII)), its authority for collecting PII, the choices, if any, individuals may have regarding how the organization uses PII, and the individual's ability to access and have PII amended or corrected if necessary. Additionally, the notice describes the PII the organization collects and the purpose(s) for which it collects that information, how the organization uses PII internally, whether the organization shares PII with external entities (including the categories of those entities and the purposes for such sharing), whether individuals have the ability to consent to specific uses or sharing of PII, how individuals may obtain access to PII, and how the PII will be protected.

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 do have the opportunity and right to decline to provide information. Veteran patients are asked if they want to enroll in the VA Home Telehealth Program by the VA Care Coordinators. Confirming they are willing to participate in the program justifies the gathering of the information within the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) system. ~~Individuals who decline will not be enrolled in the program.~~

No penalty or denial of service is attached; individuals who decline will not be enrolled in the program.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Participating in the VA Home Telehealth Program requires Veterans to provide information directly to the RPM/HT-C system by using medical devices or telephones located in their home. If a Veteran does not want to provide information, they only need to dis-enroll from the Home Telehealth program. If they decline to include information, or any portion of information, then the individuals are not enrolled in the program.

Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed, and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR. Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing.

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 Privacy Officer (PO) 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: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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: There is a risk that individuals who provide information to the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System will not know how their information is being shared and used within the Department of Veterans Affairs.

Mitigation: This PIA and the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System enrollment process serve to notify individuals of how information is handled by Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) system. The Home Telehealth -Cognosante Privacy Policy covers how the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System will collect, use, disclose, transfer, and store your information. Additionally, Figure 1 (below) provides a screen shot of the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System and serves to notify individuals of how information is handled by the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) system. Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) provides easy to follow user manuals consisting of a written guide and the associated images which explain operating, installation, and maintenance instructions for patients and staff.

Written notice is provided through the VHA Notice of Privacy Practice (NOPP) which explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-

Veterans receiving care are provided the notice at the time of their encounter.
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

A Veteran can request access their information captured in the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) system. To do so, a Veteran may ask their clinical health care provider to provide the Veteran instructions for receiving the information captured in the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) system. This information is detailed in 1.1.

In accordance with the System of Records Notice (SORN) Patient Medical Records–VA (24VA10A7), individuals seeking information regarding access to and contesting of VA medical records may write, call, or visit the last VA facility where medical care was provided. Veterans and other individuals may request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office. VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access. VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records. Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative (COR) to obtain information upon request.
In accordance with SORN 173VA005OP2, *VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP)*, individuals seeking information regarding access to and contesting of records in this system may write the Director of VA Connected Health, VHA Office of Informatics and Analytics, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420

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

The Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) 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?

The Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) 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. Technical issues are handled by Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System support.

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

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

Veterans are notified verbally during enrollment and can ask questions about the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System via the portal or by contacting their clinical healthcare provider. Technical issues are handled by Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System support. This is also indicated in the SORN as described above.

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

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

Veterans enrolled in Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System contact their Care Coordinators or other Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System support staff to have their identifying information edited. In the

case of information they have input into the portal, the administrator can note it is incorrect or needs to be deleted so the database administrators can resolve the issue.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk: There is a risk that the information provided by the Veteran is inaccurate and the Veteran will not know how to correct the information.

Mitigation: Veterans will have the ability to view (read only) their RPM/HT-V historical data within the RPM/HT-V mobile application. However, veterans may still also request their data through their clinical provider. This is also published in the SORN and this PIA and Veterans are made aware in the Notice of Privacy Practices

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

Access to the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System is received through two methods. The first method is through Cognosante (RPM/HT-C) employees who have access to the portal in order to maintain the functionality of the portal Some of the cognosante employees have elevated privileges depending on their position. This access is granted through the VA access provisioning/access form (VA 9957) process. Only users with a need-to-know and a valid business need are granted access. The second method is through clinicians who are granted access to the portal in order to review patient records and provide support to the Veterans whose information is collected. Access is granted and set up in the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System by VA Lead Care Coordinators.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

The Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System is maintained by Cognosante. Cognosante is contracted by the Department of Veterans Affairs (VA) Denver Logistics Center's (DLC's) Home Telehealth (HT) Initiative to provide support and assistance to the program. The VA Cognosante contract is reviewed annually by both the Cognosante team and VA COR to ensure compliance with the performance work statement. Cognosante staff will have appropriate, authorized access to the portal as part of assigned development, maintenance, and troubleshooting duties. Cognosante personnel involved in the operations of the Home Telehealth system complete the VA Security Clearance process. The following documents are reviewed and signed annually by each team member: 1. Cognosante Employee Handbook Acknowledgement Form, 2. Cognosante Non-Disclosure Agreement, 3. VA Contractor Rules of Behavior.

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.

Three roles have been implemented to provide access to the system:

1. Care Coordinator – This is the most basic of the roles which gives the VA care coordinator access to the system to review their patient panel.

2. Site Lead – This is the next higher role which allows for the management of Care Coordinator access.

3. VISN Lead – This is the highest role which allows for the management of administrative access for management and maintenance of the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) information system. Administrative access is not used for typical use of the Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) information system.

8.2a. Will VA contractors have access to the system and the PII?

Yes, contractors will have access to the system and the PII. The Remote Patient Monitoring / Home Telehealth - Cognosante (RPM/HT-C) System is maintained by the prime contractor Cognosante. Cognosante is contracted by the Department of Veterans Affairs (VA) Denver Logistics Center's (DLC's) Home Telehealth (HT) Initiative to provide support and assistance to the program.

8.2b. What involvement will contractors have with the design and maintenance of the system?

The VA Cognosante contract is reviewed annually by both the Cognosante team and VA COR to ensure compliance with the performance work statement. Cognosante staff will have appropriate, authorized access to the portal as part of assigned development, maintenance, and troubleshooting duties. Cognosante personnel involved in the operations of the Home Telehealth system complete the VA Security Clearance process.

8.2c. Does the contractor have a signed confidentiality agreement?

Yes, the contractor has a signed confidentiality agreement. Confidentiality information is reviewed via the Cognosante Employee Handbook and a Cognosante Employee Handbook acknowledgment form is signed by every team member. In addition, every team member reviews and signs the VA Contractor Rules of Behavior.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

Yes, the contractor has an implemented Business Associate Agreement for applicable PHI.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Yes, the contractor does have a signed non-Disclosure Agreement which is reviewed and signed annually by each team member.

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.

Team members must complete the following Security Awareness and Training Policy which mandates that:

1. All Cognosante employees shall complete Cognosante-mandated security awareness training within 30 days of being hired and complete refresher training on an annual basis.

2. Temporary access to Cognosante information systems and/or information in electronic format shall not be granted to new Cognosante personnel until the user has read and indicated their acceptance by signing the Cognosante Employee Handbook Acknowledgement Form and Cognosante Non-Disclosure Agreement.

3. All Cognosante subcontractors with access to Cognosante information systems and/or information in electronic format shall complete security awareness training when hired and complete refresher training on an annual basis.

4. All Cognosante personnel with access to PII/PHI or administrative access to information systems shall complete additional role-based training commensurate with their security responsibilities.

5. All security awareness and training activities shall be documented, tracked, and monitored for compliance. Security awareness and training will be an ongoing activity at Cognosante and will be conducted in concert with the Cognosante Training Program. Team members must also complete the following VA training courses on an annual basis:

1. VA Privacy and HIPAA Training

2. VA Privacy and Information Security Awareness Training.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

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

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Classification = Moderate, IOC Date = 9/30/2025

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. ***(Refer to question 1.8 of the PTA)***

Yes, VA Enterprise Cloud (VAEC) AWS government is the system utilized. RPM/HT-C is a Software as a Service (SaaS). which utilizes Infrastructure as a Service (IaaS).

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

The Host Cloud Service Provider is VA Enterprise Cloud (VAEC). The contract # is C03 36C79123D0002 and VA has ownership rights over data collected by the information system, including PII and PHI.

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.

Yes ancillary date will be collected. Any ancillary data collected by the CSP would be through VAEC owned and managed accounts and that ancillary data would be owned by VA.

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.

RPM/HT-C has no purview over the VAEC contract. However, they are accountable for the security and data held within their purview per the shared responsibility model referenced here: Cybersecurity in the VAEC (sharepoint.com)

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).

No RPA is in use in conjunction with PII/PHI within this information system.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2025.03.28 15:34:18 -04'00'

Privacy Officer, Nancy Katz-Johnson

STUART CHASE

Digitally signed by STUART CHASE
Date: 2025.03.31 08:01:05 -04'00'

Information Systems Security Officer, Stuart Chase

ELLEN HANS (Affiliate)

Digitally signed by ELLEN HANS (Affiliate)
Date: 2025.03.31 08:13:29 -04'00'

Information Systems Owner, Ellen Hans

APPENDIX A-6.1

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

Written notice is provided through the VHA Notice of Privacy Practice (NOPP) which explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter. https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)