Privacy Impact Assessment for the VA IT System called:

Home Telehealth – Cognosante (HTH-Cognosante)

Veterans Health Administration

VHA Office of Connected Care – VHA Telehealth Services

Date PIA submitted for review:

10/14/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dennis Lahl	dennis.lahl@va.gov	202-461-7330
Information System Security Officer (ISSO)	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?" and will be published online to accompany the PIA link.

The Home Telehealth - Cognosante system is an Information System deploying the AMC (Advanced Monitored Caregiving, Inc.) Health CareConsole system that allows clinical health care providers to review patient health information (PHI) provided by Veterans and Care Coordinators from the Veterans' homes.

This is collectively referred to as the 'system', and what Department of Veterans Affairs (VA) classifies as a Medical Device Data System (MDDS). This system is a collection of vendor servers physically located behind the VA perimeter and is categorized referred to as the Home Telehealth - Cognosante system. This is in support of the mission essential Veterans' Health Administration (VHA) Nationwide Home Telehealth (HTH) program. The Home Telehealth - Cognosante system is used by VA Care Coordinators to monitor patient health information and responses to comply with Disease Management Protocols (DMPs).

Overview

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

1 *General Description*

A. *The IT system name and the name of the program office that owns the IT system.*

Please provide response here

The Home Telehealth - Cognosante system is a Home Telehealth (HTH) Program located within the Department of Veterans Affairs (VA) Veterans' Health Administration (VHA) Office of Telehealth Services.

B. *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*

Please provide response here

VHA's Office of Telehealth Services uses information and telecommunication technologies to provide health care services in situations in which the patient and practitioner are separated by geographical distance. These telehealth technologies enable VHA to target care and case management to improve access to care, improving the health of Veterans. Store-and-Forward (asynchronous) telehealth, which allows for the capture and storage of clinical information (e.g., data, sound, image) commonly used in radiology, dermatology, and ophthalmology. Store-and-forward telehealth information can be stored in multimedia formats and evaluated later.

C. *Indicate the ownership or control of the IT system or project.*

Please provide response here

The Home Telehealth - Cognosante system is physically hosted at two VA Data Centers:

• VA Austin Information Technology Center (AITC) Data Center in Austin, TX

• VA Hines Information Technology Center (HITC) Data Center in Hines, IL
Management and control of the HTH-Cognosante information system within the VA hosted environment is maintained by HTH-Cognosante.

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

Please provide response here

The number of individuals is determined by the enrollment of Veteran patients by VA Care Coordinators. At this time, we have 11K active patients and 30K 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.

E. A general description of the information in the IT system and the purpose for collecting this information.

Please provide response here

The Home Telehealth - Cognosante 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).

The Home Telehealth - Cognosante system operates under the following system authority: Title 38, United States Code, Section 501(b)
The following information describes sharing conducted by the system and includes a general description of the modules and subsystems, where relevant, and the functions. No cloud technology will be used at any time.

Internal Sharing:

1) VA VistA

a) Reason why information is shared/received with the specified program or IT system:
Depending on your clinical workflow, periodic adjustments to the patient information may need to flow back and forth between VistA and Home Telehealth - Cognosante system.
b) List the specific information types that are shared/received with the Program or IT system:
Information commonly updated during a patient's enrolled state are medication, address and contact information.
c) Method of transmittal:
The preferred integration approach is a Patient Visit Update (ADT- A08) message in either direction.

2) VA Austin Data Center (ATIC)

a) Reason why information is shared/received with the specified program or IT system:

The Home Telehealth - Cognosante system is physically hosted within the VA Austin and VA Hines data center.
b) List the specific information types that are shared/received with the Program or IT system:

PII, PHI, III, SPI
c) Method of transmittal:

The VA data centers will host all servers and appliances related to the CareConsole.

3) VA Hines Data Center (HITC)

a) Reason why information is shared/received with the specified program or IT system:
The Home Telehealth - Cognosante system is physically hosted within the VA Austin and VA Hines data center.

b) List the specific information types that are shared/received with the Program or IT system:
PII, PHI, III, SPI

c) Method of transmittal:
The VA data centers will host all servers and appliances related to the CareConsole.

External Sharing:

1) Home Telehealth - Cognosante system Hub
a) Reason why information is shared/received with the specified program or IT system:

The Home Telehealth - Cognosante system Hub, a home medical device, is located at the VA patient home (an external organization).

b) List the specific information types that are shared/received with the Program or IT system:

PII, PHI, III, IIHI, and SPI
c) Legal authority, binding agreement, SORN routine use, etc. that permit external sharing:

i. Patient Medical Records– VA SORN (24VA10A7);
ii. VHA/Cognosante Contract No. VA791-17-D-0001;
iii. Home Telehealth - Cognosante VA Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) Version 2.0.

d) Method of transmission and measures in place to secure data:

The Home Telehealth - Cognosante system Hub connects via Plain Old Telephone System (POTS) (using a toll-free number) and through the patient's cellular phone which is the reason for an S2S VPN between the VA and the Supporting Cellular provider facility.

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

Please provide response here

Internal Sharing:

1) VA VistA

a) Reason why information is shared/received with the specified program or IT system:
Depending on your clinical workflow, periodic adjustments to the patient information may need to flow back and forth between VistA and Home Telehealth - Cognosante system.

b) List the specific information types that are shared/received with the Program or IT system:
Information commonly updated during a patient's enrolled state are medication, address and contact information.

c) Method of transmittal:
The preferred integration approach is a Patient Visit Update (ADT- A08) message in either direction.

2) VA Austin Data Center (ATIC)

a) Reason why information is shared/received with the specified program or IT system:

The Home Telehealth - Cognosante system is physically hosted within the VA Austin and VA Hines data center.

b) List the specific information types that are shared/received with the Program or IT system:

PII, PHI, III, SPI

c) Method of transmittal:

The VA data centers will host all servers and appliances related to the CareConsole.

3) VA Hines Data Center (HITC)

a) Reason why information is shared/received with the specified program or IT system:
The Home Telehealth - Cognosante system is physically hosted within the VA Austin and VA Hines data center.

b) List the specific information types that are shared/received with the Program or IT system:
PII, PHI, III, SPI

c) Method of transmittal:
The VA data centers will host all servers and appliances related to the CareConsole.

External Sharing:

1) Home Telehealth - Cognosante system Hub

a) Reason why information is shared/received with the specified program or IT system:

The Home Telehealth - Cognosante system Hub, a home medical device, is located at the VA patient home (an external organization).

b) List the specific information types that are shared/received with the Program or IT system:

PII, PHI, III, IIHI, and SPI
c) Legal authority, binding agreement, SORN routine use, etc. that permit external sharing:

i. Patient Medical Records– VA SORN (24VA10A7);
ii. VHA/Cognosante Contract No. VA791-17-D-0001;
iii. Home Telehealth - Cognosante VA Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) Version 2.0.

d) Method of transmission and measures in place to secure data:

The Home Telehealth - Cognosante system Hub connects via Plain Old Telephone System (POTS) (using a toll-free number) and through the patient's cellular phone which is the reason for an S2S VPN between the VA and the Supporting Cellular provider facility.

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

Please provide response here

The Home Telehealth - Cognosante system is physically hosted at two VA Data Centers:
• VA Austin Information Technology Center (AITC) Data Center in Austin, TX
• VA Hines Information Technology Center (HITC) Data Center in Hines, IL

Use of the HTH-Cognosante information system and PII is maintained consistently between sites through adherence to the VA Authorization and Accreditation SOP for ATO continuous monitoring; the same controls are implemented at both sites. Additionally, database replication between the primary and backup sites occurs at a regularly scheduled interval to ensure PII is maintained and up to date in both locations.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

Please provide response here

Patient Medical Records– VA SORN (24VA10A7)

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

Please provide response here

This system is not in the process of being modified and is not using cloud technology. It is on premise at AITC and HITC.

D. System Changes

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

Please provide response here

This will not result in circumstances that require changes to business processes.

K. Whether the completion of this PIA could potentially result in technology changes
Please provide response here

Completion will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Other Unique Identifying Information include: Primary Language, Health data (medications, diet, pain, mood). Biometric information (glucose meter, blood pressure, weight, etc.), EDIPI (Electronic Data Interchange Personal Identifier)

PII Mapping of Components (Servers/Database)

HTH-Cognosante Information System consists of one key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by HTH-Cognosante Information System 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VA Census and Survey Data	Yes	Yes	PII/PHI - Patient First and Last Name, 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 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 va.gov firewall.

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

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

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

VA VistA Records: The records include information concerning current and former employees, applicants for employment, trainees, contractors, sub-contractors, contract personnel, students, providers and consultants, patients and members of their immediate family, volunteers, maintenance personnel, as well as individuals working collaboratively with VA.

VA Patient Medical Records:
1. Veterans who have applied for health care services under Title 38, United States Code, Chapter 17, and members of their immediate families.
2. Spouse, surviving spouse, and children of Veterans who have applied for health care services under Title 38, United States Code, Chapter 17.
3. Pensioned members of allied forces provided health care services under Title 38, United States Code, Chapter I (i.e., Care Coordination Clinician).

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 significant 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 patient data, the data is transmitted into the Home Telehealth - Cognosante 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 Home Telehealth - Cognosante system portal develops the following reports:
• Enrolled/Active Report
• Patient Report for an Interactive Voice Response (IVR) Survey
• Patient Status Report
• New Patient Referral Report
• Priority Alert Readings
• Program/Patient Reports
• Non-Responder Reports

HTH-Cognosante CareConsole (CareConsole)

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.

Please provide response here

Data is collected from sources other than the individual in order to maintain the integrity of the data as well as support traceability.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

Please provide response here

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

1.3 How is the information collected?

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

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

VA VistA Records: Records are retrieved by name, social security number or other assigned identifiers of the individuals on whom they are maintained.

VA Patient Medical Records: Records are retrieved by name, social security number or other assigned identifiers of the individuals on whom they are maintained.

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 Home Telehealth - Cognosante 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 Home Telehealth - Cognosante system customers.

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

Please provide response here

Not Applicable. All information is recorded in CareConsole using HL7 integration between VistA/Cerner and the HTH-Cognosante information system (CareConsole).

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

The Home Telehealth – Cognosante 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 on Veterans.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Please provide response here

Not Applicable. The HTH-Cognosante information system does not use a commercial aggregator.

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

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

The VA Home Telehealth Contract # VA791-17-D-0001 issued to 1Vision, LLC, effective 2/1/2017 and novated to HMS on 8/14/2019, and then novated to Cognosante on 6/4/2020 authorizes Cognosante. to collect and process the information related to VA home telehealth patients. The data is provided by VA. The Home Telehealth - Cognosante system operates under the following system authority: Executive Order 9397-Numbering System for Federal Accounts Relating to Individual Persons; Title 38, United States Code, Section 501(b); Patient Medical Records– VA SORN (24VA10A7), October 2, 2020.

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> Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: 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.

Mitigation: In order to mitigate the privacy risks associated with the use of mobile devices, Home Telehealth - Cognosante system has developed a mobile application for Mobile Device. The Home Telehealth - Cognosante system CareConsole Mobile application incorporates the latest in mobile smartphone and tablet technology on the Android and Apple operating system platforms. Home Telehealth - Cognosante system is the first phase of the overall migration of technology stack to virtual and big data infrastructure. Mobile and web user interfaces now leverage a reactive architecture for cross-platform and cross-browser compatibility. Home Telehealth - Cognosante system also enables cross mobile platform compatibility. The mobile applications leverage a modular plugin architecture for easy integration of wireless Bluetooth sensors. Home Telehealth - Cognosante 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.

Section 2. Uses of the Information

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

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

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

The Home Telehealth - Cognosante system collects, uses, disseminates, creates, and maintains VA Sensitive Information for the following purposes:

Name: The patient's first name and the last name is collected as part of the new patient register process within the Home Telehealth - Cognosante 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.

Social Security Number (SSN): The patient's SSN is collected as part of the new patient register process within the Home Telehealth - Cognosante system portal. This information is a requirement for patients to answer this data element for registration.

Date of Birth (DoB): The patient's DoB is collected as part of the new patient register process within the Home Telehealth - Cognosante system portal. This information is a requirement for patients to answer this data element for registration.

Personal Mailing Address: The patient's Mailing Address is collected as part of the new patient register process within the Home Telehealth - Cognosante system portal. The patient's Zip Code is collected as part of the new patient register process within the Home Telehealth - Cognosante system portal.

Phone Number(s): The patient's phone number is collected as part of the Interactive Voice Response (IVR) passcode requirement process within the Home Telehealth - Cognosante system portal.

Emergency Contact Information: The patient's emergency contact information is collected as part of the new patient register process within the Home Telehealth - Cognosante system portal. This information is a requirement for patients to answer this data element for registration.

Gender: The patient's gender is collected as part of the new patient register process within the Home Telehealth - Cognosante system portal. This information is a requirement for patients to answer this data element for registration.

Primary Language. This is collected to provide service in the language the patient is most comfortable using, as their primary language.

Personal Email Address: The patient's email address is collected as part of the new patient register process within the Home Telehealth - Cognosante system portal. This information is a requirement for patients to answer this data element for registration.

Subjective Health Data: 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.

Biometric Information: Patient's vitals 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.

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.

Electronic Data Interchange Personal Identifier (EDIPI): The EDIPI is a unique member identifier that allows the VA to retrieve the Veteran's health record.

2.2 What types of tools are used to analyze data and what type of data may be produced?

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

Please provide response here

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 Home Telehealth - Cognosante 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 Home Telehealth - Cognosante 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.

Please provide response here

VA VistA Records: The records include information concerning current and former employees, applicants for employment, trainees, contractors, sub-contractors, contract personnel, students, providers and consultants, patients and members of their immediate family, volunteers, maintenance personnel, as well as individuals working collaboratively with VA.
VA Patient Medical Records:
1. Veterans who have applied for health care services under Title 38, United States Code, Chapter 17, and members of their immediate families.

2. Spouse, surviving spouse, and children of Veterans who have applied for health care services under Title 38, United States Code, Chapter 17.
3. Pensioned members of allied forces provided health care services under Title 38, United States Code, Chapter I (i.e., Care Coordination Clinician).

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 significant 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 patient data, the data is transmitted into the Home Telehealth - Cognosante 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 Home Telehealth - Cognosante system portal develops the following reports:
• Enrolled/Active Report
• Patient Report for an Interactive Voice Response (IVR) Survey
• Patient Status Report
• New Patient Referral Report
• Priority Alert Readings
• Program/Patient Reports
• Non-Responder Reports

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

Please provide response here

All servers and appliances will be configured to best practices prior to shipment to the VA data center, and Home Telehealth - Cognosante 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 ATO. Home Telehealth - Cognosante 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. Home Telehealth - Cognosante 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 Home Telehealth - Cognosante system is physically hosted within the VA Austin and VA Hines data centers. The Home Telehealth - Cognosante system is only accessible from within the VA perimeter (WAN) and will only be accessed by Care Coordinators. The Web-Enabled is accessible from the public Internet and is accessible to patients enrolled in the VA HTH program. The VA data centers will host all

servers and appliances related to the Home Telehealth - Cognosante 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 data center, 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.

Patients utilizing Plain Old Telephone Service (POTS) devices will authenticate to the RAS/Radius with a unique username and password assigned to each device. Authentication will utilize OAuth 2.0. After successful device initialization, a patient-specific access token gets stored on the device. Communications from the POTS device to the server is done via TLS (encrypted) and is accompanied by an access token to confirm the patient identity. The token itself is also encrypted with AES 256-bit. The RAS is physically located within the VA perimeter. The POTS device will transmit PHI (no PII) from the device to the server.

TLS 1.2 and HTTPS 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?

Please provide response here

Additional protections such as firewalls, network segmentation, ACLs, VPN, and MFA are employed to further protect SSNs.

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

Please provide response here

PII/PHI safeguarded in accordance with OMB Memorandum M-06-15 through the use of administrative controls such VA ROB and VA annual training, and 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?

Please provide response here

The Home Telehealth - Cognosante 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 signed annually by each team member:
- Cognosante Employee Handbook Acknowledgement Form
- Cognosante Non-Disclosure Agreement
- VA Contractor Rules of Behavior

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

Please provide response here

Yes; the Home Telehealth - Cognosante system HTH-Cognosante_AC_SOP-FINAL references the organization-level policy that outlines the policies and procedures regarding the correct use and management of access controls to the Home Telehealth - Cognosante system. Access controls shall be implemented on all Home Telehealth - Cognosante information systems, to include VA assigned devices with approved access to Home Telehealth - Cognosante system information to protect against loss of confidentiality, integrity, or availability.

2.4c Does access require manager approval?

Please provide response here

Yes; only those VA Care Coordinators who have a PIV card (which has been approved by the manager and VA COR) as well as HTH-Cognosante CareConsole credentials will be granted access.

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

Yes; access to all PII is monitored, tracked, and recoded by the HTH-Cognosante information system and audit records are stored and maintained within the application database.

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

Please provide response here

The Home Telehealth - Cognosante system HTH-Cognosante_AC_SOP-FINAL references the organization-level policy that outlines the policies and procedures regarding the correct use and management of access controls to the Home Telehealth - Cognosante system. Access controls shall be implemented on all Home Telehealth - Cognosante information systems, to include VA assigned devices with approved access to Home Telehealth - Cognosante system information to protect against loss of confidentiality, integrity, or availability.

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*

The Home Telehealth - Cognosante system retains the following types of information:

- Patient First and Last Name
- Social Security Number
- Date of Birth
- Patient Mailing Address
- Patient Phone Number
- Emergency Contact Information
- Gender
- Primary Language
- Personal Email Address
- Health data (medications, diet, pain, mood)
- Biometric Information (glucose meter, Blood pressure, weight, etc.)
- Integrated Control Number (ICN)
- EDIPI (Electronic Data Interchange Personal Identifier)

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted*

early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.

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)

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

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

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

Please provide response here

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.

Please provide response here

VA SORN - Policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records.
1. 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.

Please provide response here

Per *Home Telehealth - Cognosante system IT Asset Management Policy*, the Home Telehealth - Cognosante system IT team is responsible for the purchase, deployment, support, and disposal of all IT assets including, but not limited to, laptops, desktops, software, wireless access points, and peripherals. All procurements of IT assets should be conducted with the prior approval of the IT team.

Additionally, *Home Telehealth - Cognosante system Disposal of Home Telehealth - Cognosante system IT Assets Policy* states that the "disposal of devices containing protected information (e.g., hard drives) shall be done through a technical waste destruction company. Records certifying the destruction of information must be obtained and kept on record by the Home Telehealth - Cognosante system IT team. After disposal, the Home Telehealth - Cognosante system asset management tool must be updated with the details of the method used to dispose of the asset and the name of the recipient or company performing the disposal."

In the event of a redundant hard drive failure in one of the on premise HTH-Cognosante information system servers, per VA facility policy, failed or deprecated hard drives are provided to the facility for sanitization and destruction. HTH-Cognosante is prohibited from removing any media from all VA facilities.

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 ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: The Retention and Disposal information included in the VA Patient Medical Records SORN differs from that of VHA Records Control Schedule (RCS) 10-1. There is a potential privacy risk that records within the Home Telehealth - Cognosante system will be improperly retained or disposed.

Mitigation: Home Telehealth - Cognosante system strictly adheres to the Records Management Schedule to ensure that no records are maintained longer than necessary. To mitigate this risk, Home Telehealth - Cognosante system will coordinate with the VA records officer to ensure that the proposed schedule is accurate.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veteran Health Administration (VHA)	Patient identification and traceability between VA and HTH-Cognosante information systems	PII, PHI and Individually Identifiable Information (III) - Patient First and Last Name, Social Security Number, Date of Birth, Patient Mailing Address, Patient Phone Number, Emergency Contact Information, Gender, Primary Language, Personal Email Address, Health data (medications, diet, pain, mood), Biometric Information	Data is transmitted from the patient sensors to the medical device via Bluetooth. The medical device transfers the data to the servers through cellular/VA IPSec tunnel, analog modem via Plain Old Telephone

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		(glucose meter, Blood pressure, weight, etc.)	System (POTS), or WIFI. Patients may also interact with IVR (Interactive Voice Recognition). software package
Veteran Health Administration (VHA) VistA Systems	VistA patient registration and disenrollment within the HTH-Cognosante information system	Information commonly updated during a patient's enrolled state are medication, address and contact information. PII, PHI and Individually Identifiable Information (III)	The preferred integration approach is a Patient Visit Update (ADT (Admissions, Discharges, Transfers)- A08) message in either direction.
Veteran Health Administration (VHA) – VA Austin Data Center (AITC)	Hosting of HTH-Cognosante information system behind VA perimeter; primary site	PII, PHI and Individually Identifiable Information (III) -- Patient First and Last Name, Social Security Number, Date of Birth, Patient Mailing Address, Patient Phone Number, Emergency Contact Information, Gender, Primary Language, Personal Email Address, Health data (medications, diet, pain, mood), Biometric Information (glucose meter, Blood pressure, weight, etc.)	The VA data centers will host all servers and appliances related to the CareConsole. The Cognosante CareConsole is physically hosted within the VA Austin and VA Hines data centers
Veteran Health Administration (VHA) – VA Hines Data Center (HITC)	Hosting of HTH-Cognosante information system behind VA perimeter; secondary site	PII, PHI and Individually Identifiable Information (III) -- Patient First and Last Name, Social Security Number, Date of Birth, Patient Mailing Address, Patient Phone Number, Emergency Contact Information, Gender, Primary Language, Personal Email Address, Health data (medications, diet, pain, mood), Biometric Information (glucose meter, Blood pressure, weight, etc.)	The VA data centers will host all servers and appliances related to the CareConsole. The Cognosante CareConsole is physically hosted within the VA Austin and VA Hines data centers.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: 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 Home Telehealth - Cognosante 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 Home Telehealth - Cognosante System is only accessible from within the VA perimeter Wide Area Network (WAN) 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 Home Telehealth – Cognosante primary and backup datacenters and will be used to support cellular/Wi-Fi connectivity from patient medical devices.
The connections at each end are located within controlled access facilities 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 certificate number of Home Telehealth – Cognosante' s gateway cryptographic module for establishing the VPN tunnel is FIPS 140-2 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 at AITC and HITC include: 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 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Home Telehealth - Cognosante - CareConsole	VA Patient	CareConsole Hub is a home medical device which transmits Biometric/Health Check	Virtual Private Network /Internet	ISA/MOU/ VA Contract #VA791- 17-D-0001

Hub Device - Mobile App Cellular		Data/Patient Nickname (No last name).	Protocol Security (VPN/IPSEC)	
Home Telehealth – Cognosante-CareConsole - Web Enabled	VA Patient	CareConsole Web Enabled is the web-based patient accessible portal that transmits self- reported biometric and health check data, email address, username, and password.	HTTPS Web	ESCCB Ticket # 10A-PVR049 for external connection/ ISA/MOU/ VA Contract #VA791-17-D-0001
Home Telehealth – Cognosante-CareConsole Web Enabled with Modem	VA Patient	CareConsole IVR is phone-based patient accessible portal that transmits self-reported biometric and health check data, phonetic name, phone number, and passcode (PIN).	Plain Old Telephone System (POTS)	Care Coordinators assessment treatment plan note / VA Contract #VA791-17-D0001
Home Telehealth – Cognosante-CareConsole Hub device - IVR with Modem	VA Patient	CareConsole IVR is the phone-based patient accessible portal that transmits device-reported biometric and health check data, phonetic name, phone number, and passcode (PIN).	Plain Old Telephone System (POTS)	Care Coordinators assessment treatment plan note / VA Contract #VA791-17-D0001
Veteran Health Administration (VHA) - Unified Electronic Health Record (EHR)	DOD Defense Health Agency - Cerner	Patient First and Last Name, SSN, DOB, ICN, EDIPI, Biometric health data/vital signs	Group Encrypted Transport VPN -IPSec tunnel utilizing Joint Security Architecture (JSA) across MedCOI (Medical Community of Interest)	Interagency Agreement DOD DHA VA National MEDCOI ISA – ID 733

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The risk that Home Telehealth - Cognosante system data may be shared with unauthorized users or authorized users may share it with other unauthorized individuals.

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 Home Telehealth - Cognosante system information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. Home Telehealth - Cognosante 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 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

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

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

Please provide response here

Notice was provided verbally by the VA Care Coordinator conducting the onboarding/enrollment process with the patient.

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

Please provide response here

Notice has been provided to the individual before collection of the information. Notice was provided via a system of records notice published in the Federal Register: Patient Medical Records-VA SORN (24VA10A7). 2020-21426.pdf (govinfo.gov).

The notice provided is adequate because it provides effective notice to individuals regarding its 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 Home Telehealth - Cognosante system. 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.

Yes, individuals do have the right to consent to particular uses of the information. Participating in the VA Home Telehealth Program requires Veterans to provide information directly to the Home Telehealth - Cognosante 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.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Privacy Risk: There is a risk that individuals who provide information to the Home Telehealth - Cognosante system will not know how their information is being shared and used within the Department of Veterans Affairs.

Mitigation: This PIA and the Home Telehealth - Cognosante system enrollment process serve to notify individuals of how information is handled by Home Telehealth - Cognosante system. The Home Telehealth -Cognosante Privacy Policy covers how the Home Telehealth - Cognosante system will collect, use, disclose, transfer, and store your information. Additionally, Figure 1 provides a screen shot of the Home Telehealth - Cognosante system serve to notify individuals of how information is handled by the Home Telehealth - Cognosante system. Home Telehealth - Cognosante 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. Patient Medical Records– VA SORN (24VA10A7), October 2, 2020.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

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

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

Please provide response here

A Veteran has the ability to request access their information captured in the Home Telehealth - Cognosante 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 Home Telehealth - Cognosante system. This information is detailed in 1.1.

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).

Please provide response here

N/A; the HTH-Cognosante 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.

Please provide response here

N/A; the HTH-Cognosante 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 Home Telehealth - Cognosante 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 Home Telehealth - Cognosante system via the portal or by contacting their clinical healthcare provider. Technical issues are handled by Home Telehealth - Cognosante system support.

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 Home Telehealth - Cognosante system contact their Care Coordinators or other Home Telehealth - Cognosante system support staff to have their identifying information edited. In the case of information, they have input into the portal, the admin 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 System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the individual accidentally provides incorrect information or does not understand the questions they are sent and provides more information than necessary their correspondence.

Mitigation: Care Coordinators review all information input by Home Telehealth - Cognosante system participants. Veterans can review the data they have entered into the portal by logging in at any time.

Section 8. Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

Please provide response here

Access to the Home Telehealth - Cognosante system is received through two methods: First, Home Telehealth - Cognosante employees have access to the portal in order to maintain the functionality of the portal, some with elevated privileges if required for 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. Second, Clinicians are granted access to the portal in order to review patient records and provide support to the Veterans. Access is granted and set up in the Home Telehealth - Cognosante 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 Home Telehealth - Cognosante 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 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.

Please provide response here

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

1. CareCoordinator – 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 CareCoordinator access
3. VISN Lead – this is the highest role which allows for the management of Site Lead access

Administrative access for management and maintenance of the HTH-Cognosante information system is maintained by HTH-Cognosante. Administrative access is not used for typical use of the HTH-Cognosante information system.

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

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

The Home Telehealth - Cognosante 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 signed annually by each team member:

- Cognosante Employee Handbook Acknowledgement Form
- Cognosante Non-Disclosure Agreement

- VA Contractor Rules of Behavior

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Please provide response here
2. *The System Security Plan Status Date:* Please provide response here
3. *The Authorization Status:* Please provide response here
4. *The Authorization Date:* Please provide response here

5. *The Authorization Termination Date:* Please provide response here
6. *The Risk Review Completion Date:* Please provide response here
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Please provide response here

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

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

Yes, the Home Telehealth - Cognosante system has received an ATO (Authority to Operate) with conditions, for a full three years on 8/22/2022 with an expiration date of 8/21/2025. The FIPS 199 classification of the system is HIGH.

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

N/A – cloud technology is not used

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

N/A – cloud technology is not used

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

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

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

N/A – cloud technology is not used

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A – cloud technology is not used

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

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

N/A – Robotic Process Automation is not used.

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

ID	Privacy Controls
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2022.12.05 15:09:26 -05'00'

Privacy Officer, Dennis Lahl

Stuart E. Chase 3385791 Digitally signed by Stuart E. Chase 3385791
Date: 2022.12.05 15:37:30 -05'00'

Information System Security Officer, Stuart Chase

ELLEN HANS (Affiliate) Digitally signed by ELLEN HANS (Affiliate)
Date: 2022.12.01 10:59:26 -05'00'

Information System 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).

System of Records Notice
1.VA SORN (24VA10A7): Patient Medical Records–VA.a.Effective Date: 10/2/2020
b.Link to Printed Version: 2020-21426.pdf (govinfo.gov)

2.VHA Handbook 1605.4 *Notice of Privacy Practices,* September 6, 2015.

Cognosante AMC Health Privacy Policy
Privacy Policy (amchealth.com)