Privacy Impact Assessment for the VA IT System called:

Home Telehealth Reporting (HTR)

Veterans Health Administration

Patient Care Services / Connected Care

eMASS #1154

Date PIA submitted for review:

12/14/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dennis Lahl	Dennis.Lahl@va.gov	(202) 461-7330
Information System Security Officer (ISSO)	Oliver Patague	Oliver.Patague@va.gov	(408) 582-2884
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?".

Home Telehealth Reporting (HTR) is a cloud hosted web-based system sponsored by the Veterans Health Administration (VHA) Patient Care Services within the Office of Connected Care (OCC - VHA-12CC). HTR improves technology that Remote Patient Monitoring – Home Telehealth (RPM-HT) Care Coordinators use to maximize care for Veterans. The data from the tools are used by VHA to assess and improve Home Telehealth program outcomes and allows for updates to the system architecture to maintain security of Veteran data. HTR supports the Home Telehealth program in improving clinical outcomes and access to care by reducing complications, hospitalizations, and clinic or emergency room visits for Veterans who are at high risk due to chronic disease. The enhancements will help Veterans continue to live independently and spend less time at medical visits while providing the Veteran's knowledge and skills needed to self-manage their own health care needs more effectively. HTR is an integration project that validates data from multiple vendors and integrates it with VA systems, and provides tools and reporting to clinical staff using that data. It is not relied upon for daily operations or clinical care.

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

1. *General Description*

   A. *What is the IT system name and the name of the program office that owns the IT system?*

   Home Telehealth Reporting (HTR) | VHA Patient Care Services - Office of Connected Care (OCC – VHA-12CC)

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

   The business functions of HTR are as follows:

   - Provide Access to Health Care using Latest Technologies;
   - Manage Extended Non-Institutional Care Treatment;
   - Provide Local and Regional Reporting;
   - Provide National Reporting.

   The Office of Connected Care (OCC) focuses on improving health care through technology. By harnessing the latest virtual care tools, Connected Care expands the Veteran's experience beyond the traditional office visit. This makes health information and care more accessible for Veterans.

   HTR improves the use of technology by gathering the data from the devices that are used by Remote Patient Monitoring – Home Telehealth (RPM-HT) Care Coordinators used to monitor the health of a Veterans and then builds reports on the data. These reports inform the Home Telehealth vendors if the devices are working correctly or inaccurately reporting the Veteran's health information.

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

VA owned and VA Operated

2. Information Collection and Sharing

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

The expected number of individuals that will have their information stored in HTR is over 100,000. The affected individuals are Veterans and/or their dependents requiring care from the VA.

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

HTR collects information from multiple Home Telehealth vendors who provide devices that Remote Patient Monitoring – Home Telehealth (RPM-HT) Care Coordinators use to maximize care for Veterans enrolled in the Home Telehealth program. The information collected from these devices are used by VHA to assess and improve Home Telehealth program outcomes and allows for updates to the system architecture to maintain security of Veteran data. HTR is an integration system that validates data from multiple vendors and integrates it with VA systems, and provides tools and reporting to clinical staff using that data. It is not relied upon for daily operations or clinical care.

The data elements of the information collected are as follows:

- First and Last Name
- Date of Birth (DOB)
- Social Security Number (SSN)
- Integration Control Number (ICN)

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

HTR has interconnections with the following applications and information systems that are listed below:

System Name	Data Direction & Data Type	Type of Connection
Remote Patient Monitoring/ Home Telehealth - Medtronic (RPM/HT-M)	Bidirectional Receive and acknowledge HL7 Patient Data	Internal
Remote Patient Monitoring/Home Telehealth - Cognosante (RPM/HT-C)	Bidirectional Receive and acknowledge HL7 Patient Data	Internal
Health Data Repository (HDR)	Output System of Record	Internal

VHA Support Service Center (VSSC)	Output Patient Data	Internal

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

HTR is hosted at VA Enterprise Cloud (VAEC) Microsoft Azure Government (MAG) US South and East regions as Infrastructure as a Service (IaaS) and leverages VAEC General Support Services (GSS). This boundary incorporates all utilized resources, services, and security measures consistent throughout the regions.

3. Legal Authority and SORN

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

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

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

The system uses cloud technology and the SORN covers cloud usage/storage. The SORN will not require any amendments.

4. System Changes

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

No, the completion of this PIA will not result in any circumstances that would require changes to business processes.

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

No, the completion of this PIA 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. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☐ Personal Mailing Address
☐ Personal Phone Number(s)
☐ Personal Fax Number
☐ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Other Data Elements (list below)

Other PII/PHI data elements: N/A

PII Mapping of Components (Servers/Database)

Home Telehealth Reporting (HTR) consists of **two (2)** key components (servers / databases / instances / applications / software / application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **HTR** and the reasons for the collection of the PII are in the table below.

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

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
HTR SQL Server 1	Yes	Yes	First and Last Name, Date of Birth (DOB), Social Security Number (SSN), and Integration Control Number (ICN)	Track care of patients	Only System Administrators (SAs) have access to these servers containing PII. Data is encrypted at rest and in transit.
HTR SQL Server 2	Yes	Yes	First and Last Name, Date of Birth (DOB), Social Security Number (SSN), and Integration Control Number (ICN)	Track care of patients	Only System Administrators (SAs) have access to these servers containing PII. Data is encrypted at rest and in transit.

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?

The information collected by HTR is provided by Remote Patient Monitoring - Home Telehealth (RPM/HT) vendors, Cognosante (RPM/HT-C) and Medtronic (RPM/HT-M). The vendors provide devices used by Veterans enrolled in the Home Telehealth program to relay health information to the Remove Patient Monitoring – Home Telehealth Care Coordinators. The information collected by these sources are used as commercial data aggregators for reporting, trackers, and profiles etc.

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.

HTR does not interact with the individual and collects the information from the sources above for a commercial aggregator. Home Telehealth vendors gather the information from Veterans enrolled in the Home Telehealth program. HTR is an integration project that validates data from multiple vendors and integrates it with VA systems, Health Data Repository (HDR) and VHA Support Service Center (VSSC). HTR uses the information to provide tools and reporting to clinical staff using that data.

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

HTR generates reports using the information from Home Telehealth vendors which is shared with HDR and VSSC and Home Telehealth field staff.

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?

HTR information is collected via HL7 messages from the Home Telehealth vendors and stored in the database.

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

N/A

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.

Data is collected directly from the individual when enrolling in the Home Telehealth program. As the information is collected straight from the individual, the accuracy of the information is confirmed during the visit by field staff. The information received is from Home Telehealth vendors where accuracy is verified by the original source. HTR does not verify as it only receives the information via HL7 messages and is considered to be accurate.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

N/A

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

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

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:
HTR collects Personally Identifiable Information (PII) and other delicate Sensitive Personal Information (SPI) to improve clinical outcomes and access to health care. The information is collected from Home Telehealth vendors where information is collected from the individual via the Home Telehealth program. If this information were breached or accidentally released to inappropriate parties or the public, it could result in personal and/or emotional harm to the individuals whose information is contained in the system.

Mitigation:

VA is careful to only collect the information necessary to assist in the care of patients and provide an updated status to clinical health care providers. By only collecting the minimum necessary information, VA is able to better protect the Veterans information. Once collected, information is transmitted using Federal Information Protection Standard (FIPS) compliant encryption and stored in secure servers behind VA firewalls.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
First and Last Name	Used to identify the Veteran and/or Dependent (patient). Maintained to correctly report patient care provided by the Home Telehealth program.	Not used externally, only internal.
Social Security Number	Used to verify the patient's identity. Maintained to correctly report patient care provided by the Home Telehealth program.	Not used externally, only internal.
Date of Birth	Used to verify the patient's identity. Maintained to correctly report patient care provided by the Home Telehealth program.	Not used externally, only internal.
Integrated Control Number	Unique patient identifier used to verify the patient. Maintained to correctly report patient care provided by the Home Telehealth program.	Not used externally, only internal.

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?*

HTR does not utilize any tools to analyze data as the information collected is stored in the database and reports are generated and displayed using HTML tables. The reports list the data as statistics.

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.

HTR only receives and transfers the information via HL7 data exchange from Remote Patient Monitoring - Home Telehealth (RPM/HT) vendors, Cognosante (RPM/HT-C) and Medtronic (RPM/HT-M) and to Health Data Repository (HDR) and VHA Support Service Center (VSSC). Reports are generated listing data as statistics and are utilized by field staff to improve clinical outcomes and access to care.

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?

HTR uses Transport Layer Security (TLS) for data in transit and FIPS 140-2 compliant encryption for data at rest. HTR uses full disk encryption on its database and Secure Socket Layer (SSL) certificates to maintain confidentiality/integrity of data during preparation and reception of transmission.

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

SSNs do not appear in the HTR application. Reports generated by HTR do not contain any VA sensitive or PII/PHI, as all of the reports are congregated data and do not show by individual veteran.

Strict access controls are in place only allowing special permission levels to access any PII/PHI retained. Access is granted on a need-to-know basis and the system maintains rigorous logging and auditing.

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

The HTR application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how Veterans information is used, stored, and protected.

Following the NIST and VA policy guidance listed above, the Separation of Duties policy applied, allows HTR personnel to receive focused and recorded training that provides access only to the areas of the application that applies to their job task and responsibilities. HTR utilizes Role-based Access Control (RBAC) making PII/PHI controlled based predefined roles, ensuing only authorized individuals are able to access the information and does not share information externally.

HTR utilizes a thorough, multi-tiered strategy to safeguard highly sensitive data, ensuring compliance with relevant regulations and significantly reducing the risk of data breaches or unauthorized access:

Encryption:

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

Access Control:

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

Audit and Accountability:

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

Data Minimization:

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

Training:

- User Training: All personnel must complete mandatory training on data protection policies and procedures.
- Regular Updates: Training is regularly updated to include new policies or regulation changes and taken on an annual basis.

Network Security:

- Network firewalls and intrusion detection systems are used to monitor and control traffic flow, thereby preventing unauthorized access or data breaches.
- HTR can only be accessed on the VA Network and user access is granted upon successful authentication against the VA Multifactor Authentication using Single Sign On (SSOi).
- Virtual Private Network (VPN): In order to gain access to the VA Network, uses must first log onto the VPN for an added layer of security.

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

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

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

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

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

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

2.4a How is access to the PII determined?

Following the NIST Special Publication 800-53 and VA policy guidance listed in section 2.3b, the separation of duties policy applied, allows HTR staff members to receive focused and recorded training that provides access only to the areas of the application that applies to their job task and responsibilities. Elevated privilege access is requested through the Electronic Permission Access System (ePAS) and is approved by their Contracting Officer's Representative (COR) and the HTR manager.

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

All access is documented via the Electronic Permission Access System (ePAS) and training records are documented via VA Talent Management System (TMS 2.0). All VA personnel must sign the Rule of Behavior (ROB) which outlines what behaviors are allowed and not allowed on US Government computer systems.

Following the NIST 800-53 security controls, the HTR application cover security areas with regard to protecting the Confidentiality, Integrity, and Availability (CIA) of VA information systems and the information processed, stored, and transmitted by those systems. These security controls are documented in Enterprise Mission Assurance Support Services (eMASS) the GRC tool.

2.4c Does access require manager approval?

Yes, all requested access is approved by their Contracting Officer's Representative (COR) and the HTR manager via the Electronic Permission Access System (ePAS).

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

Yes, all HTR personnel must receive annual security and privacy training which is monitored, tracked and recorded via VA Talent Management System (TMS 2.0), Rules of Behavior (ROB) are signed and recorded in the VA Human Resources system, and all user accounts are reviewed on a quarterly basis by the System Owner.

The information system records access using audit trails, real-time alerts, and regular audits to monitor access to any sensitive information.

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

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

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

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

- First and Last Name
- Social Security Number (SSN)
- Date of Birth (DOB)
- Integration Control Number (ICN)

3.2 How long is information retained?

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

Health information is retained for seventy-five (75) years after the last episode of care. This retention period is required by the Department of Veterans Affairs Record Control Schedule 10-1, Items 6000.1d (N1–15–91–6, Item 1d) Health Records Folder File or CHR (Consolidated Health Record) and 6000.2b (N1–15–02–3, Item 3) Electronic Health Records (EHR).

https://www.va.gov/vhapublications/RCS10/rcs10-1.pdfh

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

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

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

Yes, HTR records are retained in accordance with the Department of Veterans Affairs Record Control Schedule 10-1 (http://www.va.gov/vhapublications/RCS10/rcs10-1.pdf).

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

In accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3).

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

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Records are securely eliminated in conformity with VA Handbook 6500.1 - Electronic Media Sanitization. This guideline mandates the destruction of high-security categorized data. Moreover, all types of electronic data and files, including but not limited to Protected Health Information (PHI), Sensitive Personal Information (SPI), and Human Resources records, are destroyed in compliance with the Department of Veterans Affairs Directive 6500, VA Cybersecurity Program, issued on February 24, 2021.

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

HTR does not use PII for testing, training or research.

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 risk of maintaining data within HTR is, the longer the time frame that information kept, the greater the risk in the information could be compromised or breached.

Mitigation:
To mitigate this risk, the system employs multiple layers of security controls, including advanced encryption, Multi-factor Authentication (MFA), and robust access management policies. Regular security audits and vulnerability assessments are conducted to ensure the data remains secure during the entire retention period. HTR strictly adheres to the Records Management Schedule, in order to ensure that no records are maintained longer than 75 years.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration (VHA) Home Telehealth - Cognosante (RPM/HT-C)	Source of Census and Survey Data	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) – First and Last Name, DOB, SSN, and ICN	HL7 exchange with Home Telehealth
Veterans Health Administration (VHA) Home Telehealth - Medtronic (RPM/HT-M)	Source of Census and Survey Data	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) – First and Last Name, DOB, SSN, and ICN	HL7 exchange with Home Telehealth
Veterans Health Administration (VHA) Health Data Repository (HDR)	Source of Census and Survey Data	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) – First and Last Name, DOB, SSN, and ICN	HTTPS push to HDR database and HL7 data exchange
Veterans Health Administration (VHA)	Source of Census and Survey Data	Personally Identifiable Information (PII), Protected Health Information (PHI), and	HL7 data exchange

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*
VHA Support Service Center (VSSC)		Individually Identifiable Information (III) – First and Last Name, DOB, SSN, and ICN	

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

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

<u>Privacy Risk:</u>

The privacy risk associated with sharing data within the Department of Veteran's Affairs (VA) is that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

<u>Mitigation:</u>

The principle of need-to-know is strictly adhered to by the Home Telehealth personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk:
The risk that HTR 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 in order to prevent unauthorized access.
- All personnel with access to HTR information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- Home Telehealth 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.

HTR does not interact with the individual, therefore, does not provide a notice directly to the individual.

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

HTR does not collect information from the individual as the information is gathered directly from the individual when they enroll in the Home Telehealth program.

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.

N/A

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.

HTR information is provided by the Home Telehealth (HT) program. Individuals provide information directly to the HT program through the use of medical devices or telephones located in their home. If the individual chooses not to provide information they only need to dis-enroll from the HT 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.

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

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Follow the format below:

Privacy Risk:
There is a risk that individuals who provide information to Home Telehealth will not know how their information is being shared and used internal to the Department of Veterans Affairs and will be unaware that the HTR system contains their information.

Mitigation:
This PIA and the Home Telehealth enrollment process serve to notify individuals of how information is handled by the Home Telehealth systems.

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.***

HTR does interact with the individual(s) directly therefore, any individual wishing to gain access to their information should contact their clinical health care provider and/or Home Telehealth Care Coordinator to provide them their information.

Each VHA Privacy Act System of Records Notice (SORN) informs individuals how to obtain access to records maintained on them in the SORN. The SORN for HTR is VA System of Records Notice (SORN) 24VA10A7 / 85 FR 62406 Patient Medical Records-VA 2020-21426.pdf (govinfo.gov).

The VHA Notice of Privacy Practices (NOPP) informs the individual(s) of their right to review and obtain copies of their health information maintained in VHA records. VHA permits individual to obtain access to or get copies of their information, and this is outlined in VHA NOPP. Individuals must submit a written request for copies of their records to the facility Privacy Officer at the VHA health care facility that provided or paid for the individual(s) care. The VHA Privacy Office at Central Office in Washington, D.C. does not maintain VHA health records, nor past military service health records. An individual can request a copy of their military service health records, by contacting the National Personnel Records Center at (314) 801-0800. The Web site is: http://www.archives.gov/veterans/military-service-records/medical-records.html

The individual may also submit a request via FOIA Requests – Freedom of Information Act (va.gov) or gain access to their records via the VA Blue Button - Get Your VA Medical Records Online | Veterans Affairs (https://www.va.gov/health-care/get-medical-records/).

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

N/A

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

N/A

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 through the Home Telehealth program to assist with the specific health care needs. Inaccurate information can be corrected by contacting their clinical health care provider and/or Home Telehealth Care Coordinator.

The VHA Notice of Privacy Practices (NOPP) informs the individual of their right to request an amendment (correction) to their health information maintained in VHA records if they believe it is incomplete, inaccurate, untimely, or unrelated to their care. The individual must submit a request in writing, specify the information that they want corrected, and provide a reason to support their request for amendment. All amendment requests are submitted to the facility Privacy Officer at the VHA health care facility that maintains their information or health records.

The individual may also submit a request via FOIA Requests – Freedom of Information Act (va.gov) or gain access to manage their records via the VA Blue Button - Get Your VA Medical Records Online | Veterans Affairs (https://www.va.gov/health-care/get-medical-records/).

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.

If the individual's request for amendment is denied, they will be notified of this decision in writing and given information about their right to appeal the decision. In response, they may do any of the following:

- File an appeal;
- File a "Statement of Disagreement" which will be included in their health record;
- Ask that their initial request for amendment accompany all future disclosures of the disputed health information.

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.

Inaccurate information can be corrected by contacting their clinical health care provider and/or Home Telehealth Care Coordinator.

The individual may also submit a request via FOIA Requests – Freedom of Information Act (va.gov) or gain access to their records via the VA Blue Button - Get Your VA Medical Records Online | Veterans Affairs (https://www.va.gov/health-care/get-medical-records/)

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

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

Mitigation:
If the individual wants to access their information, they may ask their clinical health care provider and/or Home Telehealth Care Coordinator to provide them with their information.

Section 8. Technical Access and Security

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

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

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

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

The Agency establishes privacy procedures, responsibilities, and departmental framework for incorporating privacy in the system development life cycle (SDLC) of information technology (IT) assets that store, process, or transmit VA information.

Administrative procedures are in place for the two primary types of users that access the HTR application, HTR System Administrators and VA clinical staff.

HTR System Administrator(s) access the information system in order to maintain the functionality of the system, which requires elevated privileges and is associated with their position. The access is granted through the VA onboarding process via the Electronic Permission Access System (ePAS) process. Only users with a need-to-know and a valid business need are granted access. Administrative access requires management approval, provided on a least privilege basis, and is reviewed quarterly.

VA clinical staff are granted access to the system in order to access the census and survey reports regarding Veterans enrolled in the Home Telehealth (HT) program who utilize HT technology devices. This provides the ability for HT Care Coordinators to input Quality Improvement Reports (QIR) to its vendors who provide support to the Veterans. These reports inform the vendors if the devices are working correctly or inaccurately reporting health information. Access is granted by going to the HTR application link (located on the VA network) where they are presented with a registration screen (after passing SSOi) which allows them to request access upon authorized approval. Only users with a need-to-know and a valid business need are granted access.

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 HTR application is only accessible on the VA network and only reports statistical information and does not contain personal data.

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.

There are several roles that users choose when requesting access to the application and are as follows:

- Care Coordinator – Read-only (reports only)
- Facility Administrator – Create, Read, and Update (certain criteria for users/reports)
- National Administrator – Create, Read, and Update (certain criteria for users/reports)
- Program Support Assistant – Read-only (reports only)
- Vendor – Read and Update (certain criteria for users/reports)
- VISN Administrator – Create, Read, and Update (certain criteria for users/reports)

HTR System Administrators can Create, Read, Update, and Delete.

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.

Yes, VA Contractors maintain the HTR system and those with administrative level privileges can access data in the database. All contactors involved in the operations of HTR have completed the initial and annual security and privacy training. Users with elevated privileges have undergone training unique to their specific role, and refresher training is mandatory and tracked in the Training Management System (TMS).

All VA contractors go through the VA onboarding process which includes an executed Information Protection and Risk Management Non-Disclosure Agreement (NDA).

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.

Part of the VA onboarding process is all personnel are required to take the following training courses in TMS prior to accessing the VA network:

- Course #VA 10176 - VA Privacy and Information Security Awareness and Rules of Behavior (ROB).
- Course #VA 10203 - Privacy and HIPPA Training

Users with elevated privileges are required to take additional training unique to their specific role. All training is maintained by taking refresher courses on an annual basis and tracked in TMS.

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

8.4a If Yes, provide:

1. *The Security Plan Status:*	Approved
2. *The System Security Plan Status Date:*	August 31, 2021
3. *The Authorization Status:*	Authorization to Operate (ATO)
4. *The Authorization Date:*	November 4, 2021
5. *The Authorization Termination Date:*	November 4, 2024
6. *The Risk Review Completion Date:*	October 25, 2021
7. *The FIPS 199 classification of the system:*	Moderate

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

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

N/A

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)*

VA Enterprise Cloud (VAEC) Microsoft Azure Government (MAG) Infrastructure as a Service (IaaS).

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

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

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.

N/A

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

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

N/A

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

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

N/A

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

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

Signature of Responsible Officials

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

DENNIS LAHL

Digitally signed by DENNIS LAHL
Date: 2024.01.02 10:16:05 -05'00'

Privacy Officer, Dennis Lahl

OLIVER PATAGUE

Digitally signed by OLIVER PATAGUE
Date: 2024.01.02 10:58:19 -08'00'

Information System Security Officer, Oliver Patague

ELLEN HANS (Affiliate)

Digitally signed by ELLEN HANS (Affiliate)
Date: 2024.01.02 14:22:46 -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; screen shot of a website collection privacy notice).

Not Applicable as HTR does not collect information from the individual. Information is transmitted via HL7 messages from Home Telehealth vendors who collect the information from the individual enrolled in the Home Telehealth program.

HELPFUL LINKS:

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

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

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

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

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