Privacy Impact Assessment for the VA IT System called:

**Home Telehealth – Medtronic Assessing (HTH-Med Assessing)**

VA Office of Connected Care / VHA Telehealth Services

**Date PIA submitted for review:**

July 6, 2022

**System Contacts:**

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Kamilah Jackson</td>
<td><a href="mailto:kamilah.jackson@va.gov">kamilah.jackson@va.gov</a></td>
<td>513-288-6988</td>
</tr>
<tr>
<td>Information System Security Officer</td>
<td>Katherine Vollmer</td>
<td><a href="mailto:Katherine.vollmer@va.gov">Katherine.vollmer@va.gov</a></td>
<td>605-745-2000 x2258</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Ellen Hans</td>
<td><a href="mailto:Ellen.hans@va.gov">Ellen.hans@va.gov</a></td>
<td>703-534-0205</td>
</tr>
</tbody>
</table>
Abstract

The abstract provides the simplest explanation for “what does the system do?” and will be published online to accompany the PIA link.

Home Telehealth – Medtronic Assessing (HTH – Med Assessing) utilizes a full suite of remote monitoring patient-facing platforms, i.e., medical devices/peripherals in the patient’s home, designed to collect patient biometrics and symptom data, while educating patients in their own self-care.

Remote Patient Monitoring- Home Telehealth (RPM-HT) is a national program sponsored by Telehealth Services within the Office of Connected Care (OCC), providing care management for Veterans with complex chronic conditions to enable them to live independently in their homes. This system is a vendor owned and operated system. Their assigned technology transmits electronic health information from the medical device to the Home Telehealth servers via a modem connection or Internet connection from patients home. The vendor monitors and maintains their system on the VA network.

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:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- 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.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes
- Whether the completion of this PIA could potentially result in technology changes
- 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?

HTH- Med Assessing is part of the VA Home Telehealth Program which is a national program sponsored by VA Office of Connected Care / VHA Home Telehealth Services, providing care
management for Veterans with complex chronic conditions. This system is a collection of servers, each of which supports data sent from medical devices or other applications from patient homes transmitting electronic health information. This data is transmitted through a VA provided modem connection or Internet connection, using a vendor provided Internet Service Provider (ISP). Many of these devices automate the process, dialing in automatically to the centralized servers and transmitting data on a regular basis or connecting to a predetermined URL.

The HTH- Med Assessing devices/applications used as part of this program are as follows:

1. Commander Flex: A physical device that the patient can connect to via peripheral extensions and utilize to record biometric data readings. This data is sent directly to the Omnivisor Pro database to be presented in the application interface.

2. LinkView: A physical device that the patient can connect to via peripheral extensions and utilize to record biometric data readings. The user also has the option of using video with the LinkView device. This data is sent directly to the Omnivisor Pro database to be presented in the application interface.

3. NetResponse Web: A web-based application where users log in to record biometric readings. Sends the recorded data directly to the Omnivisor Pro database to be presented in the application interface.

4. TeleResponse: A telephone system whereby patients are able to use voice capabilities to record their biometric statistics. This voice data is sent directly to the Omnivisor Pro database to be presented within the application interface.

5. Omnivisor Pro Application/Database: The database receives health check data from devices/applications. The application serves as a front-end user interface whereby authenticated are able to view patient health check data based on whether the appropriate permissions are given.

The HTH – Med Assessing system is hosted at the VA datacenters in Austin, Texas and Hines, Illinois. Medical devices transmit electronic health information from the device in the patient’s home to the HTH – Med Assessing server(s) via a VA provided VPN connection, modem connection or Internet connection. The system records health check data for patients, and patient identifiers exist in order to verify patient identities and match data with VA health records. PHI and PII are stored within the HTH-Med Assessing System. The system uses a web-based platform where VA users can access health check information via the use of a username and password.

HTH -Med Assessing operates under the authority of Title 38, United States Code, Sections 501(b) and 304. And the applicable SORN (System of Records Notice) is 24VA10A7/85 FR 62406 - Patient Medical Records-VA.

Data is sent by veteran patients using these medical devices and applications to a centrally controlled database where it can be accessed and viewed by clinicians on the VA Intranet only. Clinicians access this data via web access and log in credentials. The patient data can then be viewed by clinicians, so that they can monitor the patients’ health.

At this point, the creation of this PIA does not require that any changes be made to the business process. For technology changes, the HTH-Med Assessing database servers were upgraded to Microsoft SQL (Structured Query Language) Server 2019.

This system does not use any cloud technologies.
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://www.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 Account Information
- Health Insurance Beneficiary Numbers Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Gender
- Integration Control Number (ICN)
- Military History/Service Connection
- Next of Kin
- Other Unique Identifying Information (list below)

Other Unique Identifying Information - EDIPI (Electronic Data Interchange Personal Identifier) and Biometric health data (blood pressure, oxygen levels, vitals, etc.). Biometric health information is gathered to help provide a status of patient’s health to clinical health care providers.
### PII Mapping of Components

HTH-Med Assessing consists of five (5) key components. Each component has been analyzed to determine if any elements of that component collect PII. Two of the components map back to the HTH-Med Assessing database. The type of PII collected by HTH-Med Assessing and the reasons for the collection of the PII are in the table below.

#### PII Mapped to Components

**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.

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTH-Med Assessing internal database - Omnivisor Pro</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, SSN, EDIPI, ICN, Address, DOB, Phone Number, Email, and Biometric data</td>
<td>Identify patient for health check and treatment of veterans</td>
<td>• Encrypted in transit and at rest. • Logical access (strong authentication) controls to allow minimum necessary access. • VA user access provisioning process</td>
</tr>
<tr>
<td>TeleResponse</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>HTH-Med Assessing internal database - NetResponse Web</td>
<td>Yes</td>
<td>Yes</td>
<td>Name</td>
<td>Identify patient for health check</td>
<td>• Encrypted in transit and at rest. • Logical access (strong authentication) controls to allow minimum necessary access.</td>
</tr>
<tr>
<td>Commander Flex</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>LinkView</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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

*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?*
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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information received and maintained by the system is identification and biometric information gathered by medical devices located in the veteran’s homes. The medical devices used in the veteran’s 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 biometric data readings to complete a health check (or status of health). This could include blood pressure, weight, and other biometric data. As the device and or tools read and record patient biometric data, the data is transmitted into the Omnivisor Pro database so the data can be viewed within the application by clinicians. Collection of this data is required to assist clinicians in providing care for their patients in an efficient and effective manner. The system is a source of information as it generates a value (and in some cases an alert) based on the parameters set by clinicians.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is collected using medical devices located in the veteran’s homes and then transmitted electronically to the system housed in the VA datacenters. Patients use devices and applications, to collect via web browser, mobile application, telephone, and biometric devices and peripherals and send biometric data to the central application. The following applications/devices are used in the collection of information.
1. CommanderFlex: A physical device that the patient can connect to via peripheral extensions and utilize to record biometric data readings. This data is sent directly to the Omnivisor Pro database to be presented in the application interface.
2. LinkView: A physical device that the patient can connect to via peripheral extensions and utilize to record biometric data readings. The user also has the option of using video with the LinkView
device This data is sent directly to the Omnivisor Pro database to be presented in the application interface.

3. NetResponse Web: A web-based application where users log in to record biometric readings. Sends the recorded data directly to the Omnivisor Pro database to be presented in the application interface.

4. TeleResponse: A telephone system whereby patients are able to use voice capabilities to record their biometric statistics. This voice data is sent directly to the Omnivisor Pro database to be presented within the application interface.

5. Omnivisor Pro Application/Database: The database receives health check data from devices/applications. The application serves as a front-end user interface whereby authenticated are able to view patient health check data based on whether the appropriate permissions are given. Devices and applications utilize secure measures such as SIP (Session Initiation Protocol), HTTPS (Hypertext Transfer Protocol Secure), and IPSec (Internet Protocol Security protocol) connections to securely transfer information to the Omnivisor Pro SQL (Structured Query Language) database where data is viewable in the application interface.

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

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.

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.

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

HTH-Med Assessing takes reasonable steps to verify that PII is relevant to its intended use, complete, and current. HTH-Med Assessing utilizes hashing algorithms and checksums when sending and verifying information.

Data flows one way directly from patient devices into the HTH-Med Assessing application. Patients can directly input data themselves. HTH-Med Assessing verifies that data has been sent from an active device ID based on a device table in the HTH-Med Assessing application database.

Information is not checked for accuracy. If the clinical health care provider has questions, they will contact the veteran directly. The VA Care Coordinators review the information and monitor their patients from the information provided, and contact the patient, if needed.

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

HTH -Med Assessing operates under the authority of Title 38, United States Code, Sections 501(b) and 304.

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.

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:
The HTH-Med Assessing application collects Personally Identifiable Information (PII) and other delicate Sensitive Personal Information (SPI). If this information were breached or accidentally released to inappropriate parties or the public, it could result in personal and/or emotional harm to the individuals whose information is contained in the system.

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

HTH -Med Assessing employs a host of controls ranging from the following areas:
1. User access provisioning and review process
2. Data encrypted at rest and in transit
3. Security awareness training
4. Role based access
5. Documented security policies and procedures
6. User activity logging and review
7. Production migration approval
8. Separate test, development, and production environments
9. Control board reviews
10. Annual risk assessment
11. Vulnerability scanning management
12. Anti-virus / Malware prevention
13. Physical and environment data center controls (Austin Information Technology Center (AITC) and Hines Information Technology Center (HITC) VA data centers)

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.

HTH -Med Assessing’s innovative home telehealth solution allows health professionals to identify symptomatic information and intervene with the patient early enough to prevent unnecessary hospitalizations. Please find information on what is collected and maintained and how it is used:

Name and DOB: Patients names are maintained to help assist clinical health care providers in providing care to the correct patients.

SSN/EDIPI: Social Security Numbers are maintained to help assist clinical health care providers in providing care to the correct patients.

Phone Number: Phone numbers are collected at enrollment to serve as an identifier for Interactive Voice Recognition (IVR) connections.

Personal Mailing address/Personal Email address: These addresses are used to send additional peripheral devices or exchange/retrieve devices that need replaced.

Biometric data: Biometric information is gathered to help provide a status of patient’s health to clinical health care providers.

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

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.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

Vital Sign and biometric data are transmitted to the Omnivisor Pro software solution. The Omnivisor Pro application generates alerts based on vital sign alert settings established by the clinician.

Home Telehealth does not utilize any tools to analyze data. Biometric data is reviewed by clinical health care providers manually.

2.3 How is the information in the system secured?
   2.3a What measures are in place to protect data in transit and at rest?

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

HTH-Med Assessing utilizes encryption at rest and in transit. Additional safeguards for SSN are secure transmission over the VA internal network. Encrypted in transit and at rest. Logical access (strong authentication) controls to allow minimum necessary access, and VA user access provisioning process. VPN (Virtual Private Network) are used for communication from the home medical device to the HTH-Med Assessing servers within the VA environment.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?
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.

Data gathered and stored in the Home Telehealth system, HTH-Med Assessing, is used to help assist clinical health care providers understand the current health needs of a veteran. All personnel with access to HTH-Med Assessing receive annual privacy training and are required to sign the rules of behavior which document what behaviors are allowed and not allowed on a US Government computer system.

Access is based on the principal of least privilege access via role-based access. Documented roles and corresponding access privileges have been developed. A process where appropriate approvals for the provisioning of user access is required to be clearly documented and used. Any inappropriate use of information will be reported to the VA Program Manager.

### 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 information retained in the system is:
- Name
- Phone Number
- Email Address
- Social Security Number / EDIPI/ICN
- Date of Birth
- Home Address
- Hospital Status
- Biometric Data
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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

This question is related to privacy control DM-2, Data Retention and Disposal.

Home Telehealth information is retained for 75 years after the last episode of patient care. This retention period is required by the Department of Veterans Affairs Record Control Schedule 10-1, Item Number 6000.2 “Electronic Health Record”. [http://www.va.gov/vhapublications/RCS10/rcs10-1.pdf](http://www.va.gov/vhapublications/RCS10/rcs10-1.pdf)

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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.

This question is related to privacy control DM-2, Data Retention and Disposal.

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

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

Health information stored on electronic media is maintained for 75 years after the last episode of patient care and then destroyed in accordance with VA Handbook 6500 – Risk Management Framework for VA Information Systems – VA Information Security Program, which states that data with a security categorization of high must be destroyed. There are no paper records unless
the Care Coordinators print any information (print screen or screen capture), and then Care Coordinators at the local facility would be responsible for ensuring all paper documents with PII/PHI are shredded. The hard drives will be retained by the VA and will be physically destroyed via the VA’s media sanitization contract, i.e., shredded, and documented with a Certificate of Destruction.

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. Have policies and procedures been developed to minimize the use of PII 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 or live data for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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 the HTH-Med Assessing system is the longer the time frame that information is kept, the greater the risk is that the information could be compromised or breached.
Mitigation: Home Telehealth, HTH-Med Assessing, strictly adheres to the Records Management Schedule in order to ensure that no records are maintained longer than necessary. To mitigate this risk, data is encrypted at rest and role-based access is used to determine appropriate access. The data is also stored in VA data centers where a layered security infrastructure exists that is complemented by physical and environmental safeguards.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veterans Health Administration</td>
<td>Identify patient for health check</td>
<td>Patient data that may contain Personally Identifiable Information (PII), Protected Health Information (PHI)</td>
<td>Electronically pulled from VistA using HL7 (Health Link)7</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>VistA systems / Electronic Health Record</td>
<td>appropriate to patient and enrollment - Name, SSN, DOB, ICN, EDIPI, mailing and email address, and Phone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VA Census Survey</td>
<td>Identify patient for health check</td>
<td>PHI/PII -- Name, SSN, DOB, ICN, EDIPI, mailing and email address, and Phone</td>
<td>Transmitted securely over VA internal network</td>
</tr>
</tbody>
</table>

### 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. 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 Veteran’s 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 the HTH-Med Assessing 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 (PHI/PII) 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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared/received/transmitted with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTH-Med Assessing system: Hub Device – Cellular; Kore Networking</td>
<td>Relay data from home devices to Datacenter Servers</td>
<td>PHI- Name; Biometric/Health Check data is received from the home devices</td>
<td>VA Contract #: VA791-17-D-0004; SORN #: 24VA10A7 /85 FR 62406 - Patient Medical Records-VA</td>
<td>Site-to-site connection; Cellular</td>
</tr>
<tr>
<td>HTH-Med Assessing system: Hub Device – Cellular</td>
<td>Relay data from home devices to Datacenter Servers</td>
<td>PHI- Name; Biometric/Health Check data is received from the home devices</td>
<td>VA Contract #: VA791-17-D-0004; SORN #: 24VA10A7 /85 FR 62406 - Patient Medical Records-VA</td>
<td>Cellular</td>
</tr>
<tr>
<td>HTH-Med Assessing system: Hub Device – POTS (Plain Old Telephone System)</td>
<td>Relay data from home devices to Datacenter Servers</td>
<td>PHI- Name; Biometric/ Health Check data is received from the home devices</td>
<td>VA Contract #: VA791-17-D-0004; SORN #: 24VA10A7 /85 FR 62406 - Patient Medical Records-VA</td>
<td>Plain Old Telephone System</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------</td>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>HTH-Med Assessing system: Net Response - Web</td>
<td>Relay data from home devices to Datacenter Servers</td>
<td>PHI- Name; Biometric/ Health Check data is received from the home devices</td>
<td>VA Contract #: VA791-17-D-0004; SORN #: 24VA10A7 /85 FR 62406 - Patient Medical Records-VA</td>
<td>HTTPS Web</td>
</tr>
<tr>
<td>HTH-Med Assessing system: Tele Response – IVR (Interactive Voice Response)</td>
<td>Relay data from home devices to Datacenter Servers</td>
<td>PHI- Name; Biometric/ Health Check data is received from the home devices</td>
<td>VA Contract #: VA791-17-D-0004; SORN #: 24VA10A7 /85 FR 62406 - Patient Medical Records-VA</td>
<td>Telephony System</td>
</tr>
<tr>
<td>Veteran Health Administration (VHA) - Unified Electronic Health Record (EHR)</td>
<td>DOD Defense Health Agency - Cerner</td>
<td>Patient First and Last Name, SSN, DOB, ICN, EDIPI, Biometric health data/vital signs</td>
<td>Group Encrypted Transport VPN - IPSec tunnel utilizing Joint Security Architecture (JSA) across MedCOI (Medical Community of Interest)</td>
<td>Interagency Agreement DOD DHA VA National MEDCOI ISA – ID 733</td>
</tr>
</tbody>
</table>

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 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 information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
• HTH – Med Assessing 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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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. This question is 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.

Veteran patients are asked if they want to enroll in the Home Telehealth Program by their VA Care Coordinator. Confirming they are willing to participate in the program justifies the gathering of the information for HTH-Med Assessing. In addition, Notice was provided via a system of records notice published in the Federal Register: Patient Medical Records-VA SORN (24VA10A7).

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.
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. Participating in the VA Home Telehealth Program requires veterans to provide information directly to the HTH-Med Assessing system by using medical devices or telephones located in their home. If a veteran does not want to provide information, they only need to dis-enroll from the Home Telehealth program.

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

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

Yes, individuals do have the right to consent to particular uses of the information. Veterans are notified as part of the enrollment process how their information will be used. Enrollment constitutes consent. Participating in the VA Home Telehealth Program requires veterans to provide information directly to the HTH-Med Assessing system by using medical devices or telephones located in their home. If a veteran does not want to provide information, they only need to dis-enroll from the Home Telehealth program.

6.4 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.

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?

Follow the format below:

Privacy Risk:
There is a risk that individuals who provide information to Home Telehealth, HTH-Med Assessing, will not know how their information is being shared and used internal to the Department of
Veterans Affairs and may be unaware that HTH-Med Assessing relays information through intermediary sites.

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

## Section 7. Access, Redress, and Correction

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

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

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/](http://www.foia.va.gov/) to obtain information about FOIA points of contact and information about agency FOIA processes.

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).

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. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

VHA Directive 1605.01 outlines the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request For a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
VHA Directive1605.01 outlines the rights of the Veterans to amend to their records. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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

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

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

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

Formal redress is addressed in SORN 24VA10A7 and VHA Notice of Privacy Practices informs individuals how to file an amendment request with VHA.
7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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 information provided by the veteran is inaccurate and they may not know how to correct the information.

**Mitigation:**
VA Care Coordinators review all information inputted by HTH-Med Assessing. If the veteran wants to access their information in Home Telehealth, they may ask their VA clinical health care provider to provide their information. They may also be directed to the Release of Information Department where they receive care to request access to their information.

Section 8. Technical Access and Security

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

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

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

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?

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.
This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Access to the HTH-Med Assessing system is received through two methods: MCMS employees have access to the HTH-Med Assessing system in order to maintain the functionality of the system, some with elevated privileges if required for their position. This access is granted through the VA Onboarding process and the ePAS (electronic Permission Access System) process. Only users with a need-to-know and a valid business need are granted access.

Second, Clinicians are granted access to the system in order to review patient records and provide support to the veterans. Access is granted and set up in the Omnivisor Pro system by VA Lead Care Coordinators.

8.2 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 HTH-Med Assessing system is maintained by Medtronic Care Management Services who are contracted by the Office of Connected Care/VHA Telehealth Services to provide support and assistance to the program. The contract award number is VA791-17-D-0004. The contract award was made for one year with the option for another 4 renewable years. The contract is reviewed each year and renewed by way of a contract amendment. All MCMS 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. Non-Disclosure Agreement
2. Contractor Rules of Behavior

Team members must also complete the following TMS courses on an annual basis:
   1. VHA Privacy and HIPAA Focused Training
   2. VA Privacy and Information Security Awareness

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?
VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All personnel involved in the operations of the HTH-Med Assessing program have completed the initial and annual security and privacy training required by the contract. Users with elevated privileges have undergone training unique to their specific role.

Team members must complete the following TMS courses on an annual basis:
1. VHA Privacy and HIPAA Focused Training
2. VA Privacy and Information Security Awareness

In addition, Medtronic Care Management Services (MCMS) requires all employees to complete annual MCMS HIPAA and Security training.

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

If Yes, provide:

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

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

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

HTH-Med Assessing was granted a Full/1-Year (365-day) ATO on August 27, 2021, with an expiration date of August 27, 2022. The latest System Security Plan was signed on June 8, 2022. 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).

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.

This system does not use any cloud technologies.

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)

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

This system does not use any cloud technologies.

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.

This system does not use any cloud technologies.

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.

This system does not use any cloud technologies

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).

This system does not use any RPA technologies
# Section 10. References

## Summary of Privacy Controls by Family

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

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

KAMILAH M. JACKSON 105810
Digitally signed by KAMILAH M. JACKSON 105810
Date: 2022.07.25 07:40:05 -04'00'

Privacy Officer, Kamilah Jackson

Katherine Vollmer
Digitally signed by Katherine L. Vollmer 209764
Date: 2022.07.23 10:33:38 -06'00'

Information Systems Security Officer, Katherine Vollmer

ELLEN HANS (Affiliate)
Digitally signed by ELLEN HANS (Affiliate)
Date: 2022.07.25 10:13:28 -04'00'

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

(https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147)