Privacy Impact Assessment for the VA IT System called:

Global Telehealth Services-Virtual Health Platform

VHA Office of Research and Development

Date PIA submitted for review:

February 3, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer	Thomas J. Orler	Thomas.orler@va.gov	414-323-0942
Information System Owner	David Croall	David.croall@va.gov	314-745-3909

Abstract

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

The GTS VirtualHealth Platform is a SaaS-based Remote Patient Monitoring solution, designed to collect device-agnostic readings from remote medical devices and make the readings available to care team providers. The solution also includes video-teleconferencing and store & forward functionalities and is designed to be flexible & extensible to include a range of additional

capabilities.

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?*

The GTS VirtualHealth Platform (GTS-VP) is owned and operated by Global Telehealth Services, Inc. The purpose of the GTS-VP is to provide a common platform for enterprise organizations to conduct RPM activities, with the intention of creating cost savings, improved patient outcomes, and commonality of experience for all participants.

Hosted within Microsoft's Commercial Azure cloud, the GTS-VP is available virtually anywhere. The GTS-VP does not share any information with any other system, VA or otherwise. All sensitive information within the GTS-VP is stored within a single SQL server, which is protected using FIPS 140-2 validated cryptography, as required by FedRAMP. The GTS-VP has successfully completed the FedRAMP process and is listed as FedRAMP Ready at the Moderate risk level, which verifies the security of the system at least annually.

As a commercially available solution, the GTS-VP does not require a legal authority to operate, but under FedRAMP, the GTS-VP is managed against a lengthy list of laws and regulations, including, but not limited to all Federal Cyber Security laws, regulations and guidance, the Health Insurance Portability and Accountability Act (HIPAA), etc. Having completed FedRAMP, completing this PIA will not result in any need to adjust or alter either the platform or any GTS business operations. As a commercially available solution, no SORN is required.

The GTS-VP, and RPM in general, represent a tremendous opportunity to reshape the VA and not only how it delivers care to veterans, but the business processes by which it delivers that care. The GTS-VP will not be the source of this potential reshaping, but the tool that allows it to take place. RPM is a tool that has the potential to allow robust care to veterans to be accomplished over distance, and the GTS-VP provides a single device-agnostic platform upon which VA can take advantage of these technologies as they become available and mature enough to operate at an enterprise level. The GTS-VP can operate to include as many participants as desired by VA and can be adapted for use in most, if not all, disease conditions and in an as yet unidentified number of use cases. The GTS-VP is designed to flexibly respond to the workflows and business processes of VA without the need for system changes.

The GTS-VP operates using both web-based and mobile based access points and has three broad groups of participants. The VA care providers access the GTS-VP through a web portal, using multifactor authentication (MFA). From this portal, providers can enter veterans into the system, prescribe specific assessments and monitoring to be completed by the veterans, initiate and manage telehealth visits with veterans and monitor veteran health activities over time. Veterans access the GTS-VP from a mobile device (smartphone, tablet, etc.) and the GTS VirtualHealth patient application. This mobile app is available in the Apple Store and Google Play and must enter an invitation code generated by the system and issued at the request of the provider. Veterans also use MFA to access the app. The final group of participants are the family and friends of Veterans, who are invited to the platform by the veteran and are referred to in the GTS-VP as Companions. Companions access the GTS-VP through the GTS SmartShare app, also available through the Apple Store and Google Play, which also uses MFA for access. Veterans have dynamic access over the ability for Companions to access any information.

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☐ Social Security Number
☐ Date of Birth
☐ Mother's Maiden Name
☐ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial 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)

Personal Health Information collected through Remote Patient Monitoring and assessments.
The GTS-VP can generate a unique identifier for the veteran, or VA's care teams can enter any unique identifier to be used within the system.

PII Mapping of Components

The GTS-VP consists of several key components, but only includes two (2) database components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the GTS-VP and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
SQL Server	Yes	Yes	Medical device readings and demographic information	Medical data collected for Veteran treatment	FIPS 140-2 validated Encryption

Vidyo Database	**No**	**No**			**FIPS 140-2 validated Encryption**

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.

The demographic information pertaining to VA Employees and Contractors (name, email address, phone number) are entered into the GTS-VP by VA Employees who are given the role of Organizational Administrator.

The demographic information pertaining to Veterans (name, email address, phone number) are entered into the GTS-VP by VA Employees and Contractors for the purpose of enrolling those Veterans into the platform.

The medical information pertaining to Veterans is entered into the GTS-VP by the Veteran through the process of collecting readings from the associated medical devices used by the Veteran or by a Veteran completing a patient assessment, as prescribed by a VA Employee or Contractor.

Medical information pertaining to Veterans, for inpatient settings, is collected by the care team, working with the Veteran.

The demographic information pertaining to Companions (name, email address, phone number) are entered into the GTS-VP by the Veteran who enters the Companion into the GTS-VP.

The use of video teleconferencing (between a Veteran and a VA Employee or Contractor) is considered PII, but teleconferences are not recorded, and no details of the participants are retained.

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.

Manual entry:
VA Employee and Contractor information
Veteran demographic information
Companion demographic information
Patient Assessments

Collection from remote medical devices:
Readings from remote medical devices are collected from Veterans when the Veteran initiates a reading from the connected device.
Readings from remote medical devices are collected from Veterans during inpatient settings are initiated by the care team from the connected device.

Video Teleconferences are initiated by the provider user.

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.

There is no way to determine whether the readings collected from the medical devices are accurate, because there is no way for the system to determine that the medical device is being used correctly. All readings are checked to determine that they match the appropriate format prior to being entered into the system. By encrypting the data from the point of collection, it limits the potential for the data being altered at any point.

Provider and patient information is not validated by GTS. GTS relies on the Federal agency with whom the patients and providers are associated to conduct adequate identification and authentication to ensure the accuracy of any PII within the GTS VirtualHealth Platform

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.

The use of the GTS-VP within VA is legally authorized to operate under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a) Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).

As a commercially hosted Software as a Service (SaaS) solution, the GTS-VP does not have a System of Records Notice (SORN).

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

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

<u>Principle of Minimization:</u> 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 privacy risks cross many of the privacy principles. The risks are listed in order and the associated mitigations are in the same order.

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

Mitigation: As listed above, the mitigations are listed in the same order as the risks.

- Collection Limitation Principle: The GTS-VP collects only those medical readings that are prescribed by the care provider. The GST-VP does not collect all data that may be available on a given medical device. The GTS-VP limits the data collected from a given medical device to those data points necessary for the care of the Veteran. In outpatient settings, medical readings can only be collected from medical devices when the Veteran specifically requests the mobile application to initiate a reading. Patient assessments are an additional way to gather information from the Veteran. These assessments must be completed by the Veteran. As such, all information collected from the Veteran is done with the knowledge and consent of the Veteran. In inpatient settings, care team members take the readings from Veterans. These activities are managed in the same manner as all inpatient activities. The Veteran has the ability to invite family members or friends to participate in the care/treatment process, through the role of Companion. Veterans have dynamic control over the access that any Companion has to the information of the Veteran.
- Data Quality Principle: Only those medical readings that are prescribed by the care provider, and therefore necessary for the treatment of the diagnoses related to the Veteran. It is the responsibility of the Customer Agency to keep demographic information related to any individuals entered into the GTS-VP is kept up to date. Readings from medical devices are time stamped and represent a point in time, negating the need to have it kept up to date. And while readings are checked to ensure that the data collected into the GTS-VP are valid readings, there is no way to check them for accuracy. The care team can set alert levels for each reading type which would enable them to be alerted if an erroneous reading should be collected.
- Purpose Specification Principle: Every user of the GTS-VP must acknowledge the purpose of the system and their responsibilities in using it, prior to being given access to the system. Medical readings collected from Veterans are used for the sole purpose of assisting the

treatment of the health of the Veteran. Medical readings may be used for research purposes to evaluate the effectiveness of Remote Patient Monitoring as it relates to cost savings, patient outcomes and VA efficiencies. The data used for these purposes are used within the platform.

- Use Limitation Principle: Every user of the GTS-VP must acknowledge the purpose of the system and their responsibilities in using it, prior to being given access to the system. Medical readings collected from Veterans are used for the sole purpose of assisting the treatment of the health of the Veteran. The use of the medical information related to studies evaluate Remote Patient Monitoring is intended to further support improved Veteran treatment and outcomes.
- Security Safeguards Principle: All data collected by and retained within the GTS-VP is encrypted with FIPS 140-2 validated cryptography. This includes data at rest as well as data in transit.
- Openness Principle: Although the care team can enter the basic demographic information of a Veteran into the GTS-VP without the permission of the Veteran, the Veteran must actively respond to the invitation. The Veteran also must actively collect readings from medical devices or fill out Patient Assessments. As such, no Veteran can have health information within the GTS-VP without his/her knowledge.
- Individual Participation Principle: Veterans have the ability to view the past 30 days of readings collected. Beyond thirty (30) days, Veterans can use the VA process for viewing and reviewing their information.
- Accountability Principle: The GTS-VP is managed under the requirements of FedRAMP. As such the GTS-VP is subject to an audit at least annually.

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.

Personal Demographic Information – All Personal Demographic Information (Name, Phone Number, Email) are only used for the purpose of allowing the individual to access the GTS-VP or to communicate with said individual.

Personal health information – All personal health information collected and stored within the GTS-VP is used for the purpose of providing medical treatment to Veterans.

Information within the GTS-VP is also used for research purposes to study the effectiveness of Remote Patient Monitoring. The

No information from or within the GTS-VP is used or available to any external parties.

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

The GTS-VP does not create or make available new information about any individual.

Providers do have the ability to create notes regarding a Veteran or attach files to the records of a Veteran.

The health information within the GTS-VP is analyzed as part of studies to determine the effectiveness of RPM as it relates to cost savings, Veteran health outcomes, etc.

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

Consistent with the requirements of FedRAMP, all information collected and/or retained by the GTS-VP is encrypted using FIPS 140-2 validated cryptography.

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

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.

The basic unit of segregation within the GTS-VP is the Organization. Organizations are created, based on the requirements of VA, to encompass small groups of Veterans and their Care Teams and to limit access of providers to only those Veterans that they directly provide treatment to.

Access to the information related to any specific Veteran is limited to those providers who have access to the organization within which the Veteran is enabled. Veterans can be associated with multiple organizations. Providers can be given access to multiple organizations but may only access one organization at any given time.

Provider users are enrolled into and managed by Organizational Administrators. Organizational Administrators are responsible for ensuring that only those individuals who require access to the information related to Veterans are able to get it.

An additional use for Veteran health information is for research to determine cost savings, improvements in patient outcomes and to find other ways to improve the lives and health of Veterans.

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

Demographic information related to the Veteran is entered into the GTS-VP by VA care provider users. This information includes the Veteran's name, phone number and/or email address. The GTS-VP can generate a unique identifier for the Veteran, or a unique identifier can be entered into the platform by the care team.

The demographic information for VA personnel includes name, phone number and/or email address.

Medical information is created by the veteran either when they take RPM readings from devices or when they manually enter information into either an assessment or for a device reading.

All information is retained within the GTS-VP indefinitely. The GTS-VP allows individuals within the system to be categorized as inactive, but information may not be deleted from the system.

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.

All information is retained within the GTS-VP indefinitely.

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.

The GTS-VP will follow the records schedule for Patient Generated Data. This is RCS-10, item numbers:

- 6010.1 – Patient/User Profile Administration or Descriptive Items
- 6010.2 – Patient Generated Health Data (PGHD) and Observation of Daily Living Data (OOLD)

- 6010.3 – Medical Assessments/Forms

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

Consistent with Question 3.2, records are not destroyed or eliminated. All records are electronic in nature and elimination / destruction involves logical removal from the electronic storage medium. When the storage medium is to be destroyed at the end of its use, physical destruction of underlying physical storage is handled by Microsoft as covered by our contract and detailed in their data destruction policies

All data from the GTS-VP (electronic, paper, etc.) are required to be destroyed/sanitized consistent with VA Directive 6500, VA Cybersecurity Program and NIST SP 800-88 rev 1.

If, at the end of any relationship between GTS and VA, and after the legal obligations for retention have been met, VA desires the information to be erased, GTS would delete the VA Instance of the GTS-VP and all backup copies.

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

GTS does not use live data for testing. GTS maintains test and demo environments where synthetic data is used for all testing.

Patient data is used for research related to the cost savings related to the use of Remote Patient Monitoring, improvements in patient outcomes and other cost saving activities.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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 privacy risks for the GTS-VP fall into two categories:

- Data minimization
- Data quality and integrity

Mitigation: The mitigations are listed in order below:

- Data minimization: The GTS-VP collects only those pieces of information requested by the providers for the treatment of the Veteran. The additional information that may be available from the medical devices are not collected.
- Data quality and integrity: Because all medical readings and assessments are time stamped, they are unchanging, which mitigates many of the risks associated with data quality over time. As an potential extension to a medical record, there are potential limits on the ability to eliminate or delete this data.

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***
N/A			

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: N/A

Mitigation: N/A

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				

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: N/A

Mitigation: N/A

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.

All users of the GTS-VP are required to acknowledge their obligations prior to accessing the system. This is covered by the Rules of Behavior, as required by FedRAMP. This is included as an attachment to this document.

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

Participation in the GTS-VP is completely voluntary. Veterans who do not wish to have their information collected and made available to their healthcare provider can choose not to participate.

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

No. Consent by the Veteran is considered to be consent for all uses of the data collected and retained within the GTS-VP.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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:
N/A – The demographic information of the veteran is provided by VA, not collected from the Veteran. The veteran has the choice with regard to whether to participate and whether to collect any

given vital reading. If the Veteran does not wish to participate in the collection and use of information, they have the option not to participate.

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/ 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.

Veterans access the GTS-VP through their registered mobile device (phone, tablet, etc.). Access requires multifactor authentication, as required by FedRAMP.

Veterans are able to see up to thirty (30) day so past readings through the mobile application.

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.

Demographic information within the GTS-VP can be changed at any time by VA personnel.

RPM readings and assessments are not able to be removed or changed.

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.

RPM readings and assessments are unable to be changed or removed.

Should any demographic information be inaccurate, it can easily be changed by participants in the system.

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.

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

Demographic information is able to be changed by participants in the system.

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

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

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

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

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

Follow the format below:
N/A – Veteran demographic information is provided by VA, not the veteran. Additionally, if the demographic information is inaccurate, it can be changed within the system. Because readings and assessments can't be changed, there is no need for redress.

Section 8. Technical Access and Security

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

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

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.

Privileged users of the GTS-VP are required to request access through an Access Request form. All other users of the GTS-VP are entered into the system by Care team members or Veterans, see below.

The only privileged role within the GTS-VP that is filled by VA personnel is the role of Organizational Administrator. The individuals who fill this role are responsible for filling other roles.

Organizational Administrators are responsible for entering Provider Users and Device Managers into the GTS-VP.

Provider Users are responsible for entering Veterans (Patients) into the GTS-VP.

Veterans (Patients) have the ability to invite family or friends to participate in the care process. This role is called Companion.

All users within the GTS-VP are required to use Multi-factor Authentication (MFA) to gain access.

Veterans (Patients) establish a link to the GTS-VP through a specific mobile device. This is coupled with a PIN to gain access.

All other users within the GTS-VP use MFA enabled by Okta. This includes but is not limited to the use of Personal Identity Verification (PIV) credentials.

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 extent to which VA contractors are users within the GTS-VP is determined by each VA organization. These individuals use the GTS-VP consistent with their participation in the care teams providing medical treatment to Veterans. As such, any oversight of their activities is managed by the appropriate components of VA.

As providers of a Software as a Service (SaaS), GTS employees and service providers are not considered VA contractors.

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.

It is the responsibility of VA to ensure that all users receive the appropriate security and privacy training prior to being given access to the GTS-VP.

Consistent with FedRAMP requirements, all GTS employees and service providers complete security and privacy awareness training, prior to being given access to the system.

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.***

27 APR 2019

The GTS-VP received authorization and accreditation for use in VA as a Software as a Service (SaaS) service on

The GTS-VP has completed the process for FedRAMP authorization and is currently listed as FedRAMP Ready. This approval was granted on 03 JAN 22. As such, all security documentation has been completed and reviewed by a FedRAMP certified third party assessment organization (3PAO). Consistent with FedRAMP requirements, the GTS-VP is audited at least annually. This becomes the effective date for all security documentation to 3 JAN 22.

The GTS-VP is also completing the VA process to be granted an Authority to Operate (ATO), which is due to be completed by 01 JUN 22.

The FIPS 199 categorization of the GTS-VP is moderate.

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.

The GTS-VP has been approved by FedRAMP as FedRAMP Ready as of 03 JAN 22, as a SaaS solution.

The GTS-VP is also completing the VA process to be granted an Authority to Operate (ATO), which is expected to be complete on 01 JUN 22.

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.

The data within the GTS-VP is the property of VA and/or the Veteran.

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.

The GTS-VP does not collect any ancillary information.

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.

The roles and responsibilities of all users of the GTS-VP are delineated in the Rules of Behavior included as an attachment to this document. The customer (VA) responsibilities are delineated in the FedRAMP Customer Responsibility Matrix (CRM) required as part of FedRAMP. These responsibilities include that VA and VA personnel follow VA policies and procedures as their activities related to:

- Access Control
- Assessment, Authorization and Monitoring
- Identification and Authentication
- Incident Response
- System and Services Acquisition

Consistent with the requirements of FedRAMP, GTS is responsible for successfully completing all actions and activities necessary to maintain this status.

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. The GTS-VP does not make any use of RPA capabilities.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2022.03.18 09:18:13 -04'00'

Privacy Officer, Nancy Katz-Johnson

Thomas J. Orler 178546

Digitally signed by Thomas J. Orler 178546
Date: 2022.03.22 12:01:41 -05'00'

Information Security Systems Officer, Thomas J. Orler

DAVID CROALL

Digitally signed by DAVID CROALL
Date: 2022.03.28 12:04:22 -04'00'

System Owner, David Croall

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).

Rules of Behavior for External Users

You must conduct only authorized business on the system.

Your level of access to systems and networks owned by GTS is limited to ensure your access is no more than necessary to perform your legitimate tasks or assigned duties. If you believe you are being granted access that you should not have, you must immediately notify the GTS Operations Center *Enter phone number*.

You must maintain the confidentiality of your authentication credentials such as your password. Do not reveal your authentication credentials to anyone; a GTS employee should never ask you to reveal them.

You must follow proper logon/logoff procedures. You must manually logon to your session; do not store you password locally on your system or utilize any automated logon capabilities. You must promptly logoff when session access is no longer needed. If a logoff function is unavailable, you must close your browser. Never leave your computer unattended while logged into the system.

You must report all security incidents or suspected incidents (e.g., lost passwords, improper or suspicious acts) related to GTS systems and networks to the GTS Operations Center *Enter phone number*.

You must not establish any unauthorized interfaces between systems, networks, and applications owned by GTS.

Your access to systems and networks owned by GTS is governed by, and subject to, all federal laws, including, but not limited to, the Privacy Act, 5 U.S.C. 552a, if the applicable CSP Name system maintains individual Privacy Act information. Your access to CSP Name systems constitute your consent to the retrieval and disclosure of the information within the scope of your authorized access, subject to the Privacy Act, and applicable state and federal laws.

You must safeguard system resources against waste, loss, abuse, unauthorized use or disclosure, and misappropriation.

You must not process U.S. classified national security information on the system.

You must not browse, search or reveal information hosted by GTS except in accordance with that which is required to perform your legitimate tasks or assigned duties.

You must not retrieve information, or in any other way disclose information, for someone who does not have authority to access that information.

You must not publish or post organizational information on public websites social media/networking sites.

You must ensure that Web browsers use Secure Socket Layer (SSL) version 3.0 (or higher) and Transport Layer Security (TLS) 1.0 (or higher). SSL and TLS must use a minimum of 128-bit, encryption.

You must ensure that your web browser is configured to warn about invalid site certificates.

You must ensure that web browsers warn if the user is changing between secure and non-secure mode.

You must ensure that your web browser window used to access systems owned by GTS is closed before navigating to other sites/domains.

You must ensure that your web browser checks for a publisher's certificate revocation.

You must ensure that your web browser checks for server certificate revocation.

You must ensure that web browser checks for signatures on downloaded files.

You must ensure that web browser empties/deletes temporary Internet files when the browser is closed.

By your signature or electronic acceptance (such as by clicking an acceptance button on the screen) you must agree to these rules.

You understand that any person who obtains information from a computer connected to the Internet in violation of her employer's computer-use restrictions is in violation of the Computer Fraud and Abuse Act.

You agree to contact the GTS Chief Information Security Officer or the GTS Operations Center *Enter phone number* if you do not understand any of these rules.

ACCEPTANCE AND SIGNATURE

I have read the above Rules of Behavior for External Users for CSP Name systems and networks. By my electronic acceptance and/or signature below, I acknowledge and agree that my access to all GTS systems and networks is covered by, and subject to, such Rules. Further, I acknowledge and accept that any violation by me of these Rules may subject me to civil and/or criminal actions and that GTS retains the right, at its sole discretion, to terminate, cancel or suspend my access rights to the GTS systems at any time, without notice.