Privacy Impact Assessment for the VA IT System called:

Telehealth Management Platform (TMP)
Software Product Management (SPM)
Veteran Health Administration (VHA)

Date PIA submitted for review
09/21/2022

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>Jacquelyn R Filkins</td>
<td><a href="mailto:Jacquelyn.Filkins@va.gov">Jacquelyn.Filkins@va.gov</a></td>
<td>607-664-6964</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Thomas J Orler</td>
<td><a href="mailto:Thomas.orler@va.gov">Thomas.orler@va.gov</a></td>
<td>708-938-1247</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Stefano Masi</td>
<td><a href="mailto:Stefano.masi@va.gov">Stefano.masi@va.gov</a></td>
<td>860-681-9927</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.

The U.S. Department of Veterans Affairs (VA) Veterans Benefits Administration (VBA) provides benefits and services to eligible Veterans and their dependents. The Customer Relationship Management (CRM) Telehealth Management Platform (TMP) program will develop an application that is built upon the Microsoft Consumer Off-the-Shelf (COTS) CRM solution, which has been optimized specifically for VHA’s Office of Connected Care Telehealth. TMP provides VHA Clinical Schedulers and Providers with a single interface to manage Telehealth appointments, Provider credential validation, and control over the VA Video Connect (VVC) clinical video teleconferencing solution by automatically issuing uniform resource locator (URL) links for the Patient and Provider with associated PINS for one-touch video connectivity.

The TMP software has bi-directional secure interfaces to the VA Veterans Information System and Technology Architecture (VistA) Computerized Patient Record System (CPRS) and VistA Scheduling Enhancements (VSE) for synchronous read/write capability to all required resources to coordinate Providers’ calendars, room resources, and video service/equipment and required ancillary equipment availability and scheduling. TMP provides issuance of Telehealth appointment notifications both electronically and by letter to the patient as well as automated email reminders. TMP also maintains a record of all scheduled encounters and clinic codes for the purposes of analytics for reporting metrics, such as system utilization and resource availability for streamlining and efficiency enhancements.

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 PHI 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 TMP application is owned by U.S. Department of Veterans Affairs (VA) Veterans Health Administration (VHA). The CRM implementation for the TMP program provides an application that is developed and built upon the Microsoft Consumer Off-the-Shelf (COTS) CRM solution, which has been optimized specifically, for the Veteran Health Administration’s (VHA’s) Office of Connected Care Telehealth.

TMP provides VHA Clinical Schedulers and Providers with a single interface to manage Telehealth appointments, perform provider credential validation, and provide control over VA Video Connect (VVC) clinical video teleconferencing solution by automatically issuing URL links for the Patient and Provider with associated PINS for one-touch video connectivity.

The expected number of individuals who choose to utilize the TMP application is conditional on trends in Veteran participation with VA telehealth services. VA’s commitment to investments within its Connected Care program will undoubtedly promote participation growth and, as such, data demands on TMP.

PII/PHI information stored in TMP is used to prepare various management, tracking, and follow-up reports that are used to assist in the management and operation of the healthcare facility, and the planning, scheduling, and delivery of patient medical care.

The Telehealth Management Program (TMP) integrates with Veterans Health Information Systems and Technology Architecture (VistA) to schedule, cancel or update appointments in support of Telehealth services provided by the VA. Veterans Health Information Systems and Technology Architecture (VistA) VistAWeb is a read-only intranet web application. It delivers to the client a uniform, well-defined suite of objects from the medical domain, objects such as patient, provider, progress notes, lab results, prescriptions, allergies, and imaging. Master Veteran Index (MVI) database based on the enhanced Master Patient Index (MPI) is the authoritative identity service within the VA, establishing, maintaining, and synchronizing identities for VA clients, Veterans, and beneficiaries.

TMP Application is used in various sites with Role-based Security within the application to limit user access to PII and PHI information. Customized Microsoft internal security roles are designed and employed to control all access to data stored within TMP. Contractors and VA employees are required to complete VA Privacy and Information Security Awareness and Rules of Behavior Training, and Privacy and HIPAA-focused training.

Completion of this PIA will not result in circumstances that require changes to business processes or technology changes. The VA Handbook 6517 states a public cloud service requires FedRamp certification. TMP meets this requirement as the application and associated databases are hosted in the VA Azure Cloud.
Citation of the legal authority to operate the IT system is “Title 38, United States Code, Section 501 – Veterans’ Benefits” and “SORN 58 VA21/22/28, 38 USC 1781, 1802, 1724, 1728, 1703, 1725, 1728, 1781, 1803 and Public Law 103-446 section 107”.


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:

- [x] Name
- [x] Social Security Number
- [x] Date of Birth
- [ ] Mother’s Maiden Name
- [x] Personal Mailing Address
- [x] Personal Phone Number(s)
- [x] Personal Fax Number
- [x] Personal Email Address
- [x] 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
- [x] Internet Protocol (IP) Address Numbers
In addition, the following Veteran information is also collected and/or saved:

- Date of death
- VistA station identifiers
- Corresponding other system identifiers (CORP, BRLS, etc.)
- Identity theft indicator
- Status of Government Funded Equipment (GFE) possession and connection information if equipment issues
- Virtual Meeting Space connection information (storage newly obsolete, as connection information now dynamically generated at time of scheduling)
- Time zone
- Marital status
- Deceased status
- Branch of service
- Data File Number (DFN)

### PII Mapping of Components

Telehealth Management Platform consists of 2 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Telehealth Management Platform and the functions that collect it are mapped below.

#### PII Mapped to Components

<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>MVI (Master Veteran Index)</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, SSN, DOB, Response from MIV:</td>
<td>PII/PHI for Veterans for MVI Person Search and MVI Proxy Add to VistA via Veterans Relationship Management (VRM)</td>
<td>Role-based Security within the TMP application to</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 is collected directly from the Veteran and from the Master Veterans Index (MVI) system, based on a search of the MVI.

The source for VA networked computer IP address is from BGinfo (snapshot of personal computer (PC) information) from a point of contact at the Community Based Outpatient Clinic (CBOC) site. Once stored in TMP, TMP is the source of reporting this information. The completion of this PIA does not result in circumstances that require changes to existing business processes, as the legacy version of this system was originally developed with the existing business processes already taken into account.

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

<table>
<thead>
<tr>
<th>Source</th>
<th>Yes</th>
<th>Yes</th>
<th>Role-based Security within the TMP application to limit user access to PII and PHI information</th>
</tr>
</thead>
<tbody>
<tr>
<td>VismA</td>
<td></td>
<td></td>
<td>VIMT; sent to / received from VRM; Clinical data that may contain Protected Health Information (PHI) appropriate to the Telehealth Appointments</td>
</tr>
</tbody>
</table>
Information is collected from the Veteran (on web forms and sent electronically over the Internet to project systems) and collected (queried) from the MVI system to positively identify a Veteran.

Within the scheduling function of TMP, a Veteran Search screen is initiated by VA staff by requesting information from the Veteran during the scheduling process.

Either an Electronic Data Interchange Personal Identifier (EDIPI) is entered (required, but not available to Veteran or staff, so not used) or the combination of first name (required), middle name, last name (required), suffix, social security number (required), phone, and date of birth (required) are entered.

TMP initiates or opens a Patient record within the system, if one exists. Data is brought in from the MVI, as described above.

Veteran’s e-mail address (necessary for VMR and GFE usage) is entered and/or verified.

Veteran’s phone number(s) is/are entered and/or verified (home, mobile, business).

Veteran’s possession of GFE for video visits is entered/verified. Tablet type and connection information are entered/verified.

The patient record is saved within the system.

The source for VA networked computer IP address is from BGinfo (snapshot of PC information) from a point of contact at CBOC site. Information is stored on TMP Technology record within the system.

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 the 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.

Information is collected directly from the Veteran. Information obtained from the MVI is verified with the Veteran at the time of scheduling to assure accuracy within the TMP system.

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

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

The TMP application complies with the following Federal regulations and/or Departmental policies and guidelines, as follows:

- Title 38, United States Code, Section 501-Veterans’ Benefits
- System of Records 150VA19-E8-28183– Administrative Data Repository- VA
- Title 38, United States Code, Section 501- Veterans’ Benefits
- Joint Commission National Patient Safety Goals- Goal 1: Improve the accuracy of patient identification
- VHA Directive 1906- Data Quality Requirements for Healthcare Identity Management and the Master Veterans Index Functions
- VHA Directive 2009-021 Data Entry Requirements for Administrative Data
- VHA Directive 2006-036 Data Quality Requirements for Identity Management and the Master Patient Index Functions
- VHA Directive 2007-037 Identity Authentication for Health Care Services
- VA Directive 6300, Records and Information Management
- SORN 168VA005/86 FR 6975, Health Information Exchange
- SORN 173VA005OP2/86 FR 61852, Cloud usage and storage
- SORN 58 VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records

The Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a), Executive Order 9397 gives authority to collect the SSN, and VA policy provides privacy protections for employees or customer information that VA or its suppliers maintain in a System of Records (SOR). A SOR is a file or application from which personal information is retrieved by an identifier (e.g. name, unique number or symbol). Data maintained in a SOR must be
managed in accordance with the requirements of the Privacy Act and the specific provisions of the applicable SOR Notice. Each SOR Notice is to be published in the Federal Register.

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

Privacy Risk: TMP collects Personally Identifiable Information (PII) and other highly delicate Personal Health Information (PHI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, 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 identify the party needing medical assistance. By only collecting the minimum necessary information, the VA is able to better protect the individual’s information.

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.

Information collected or maintained includes the following data elements:
Name: Veteran’s identification
- Social Security Number: Used to verify Veteran identity and as a file number for Veteran
- Name
- Date of Birth: Used to verify Veteran identity
- Mailing Address: Used to correspond with the Veteran
- Zip Code: Part of the mailing address
- Phone Number(s): Used to correspond with the Veteran
- Fax Number: Used to correspond with the Veteran
- Email Address: Used to correspond with the Veteran
- Emergency Contact Information (Name, Phone Number, etc. of a different individual): used in emergencies to contact the Veteran
- Internet Protocol (IP) Address Numbers: Used to correspond with agents assisting the Veteran
- Gender
- Data File Number (DFN)
- Integration Control Number (ICN)
- Deceased status
- Date of Death
- VistA Station identifies
- Corresponding other system identifies (CORP, BRLS, etc)
- Identity theft indicator
- Status of Government Funded Equipment (GFE) possession and connection information if equipment issues
- Virtual Meeting Space connection information
- Time Zone
- Marital status
- Branch of service

The only external use of the information is the sending of an e-mail notification to the Veteran, which is an appointment reminder and, in the case of the use of a Virtual Medical Room, provides connection information for the video visit. The e-mail address is supplied by the Veteran at the time of scheduling and is verified with each scheduled event. No PII or PHI is included in the e-mail message, just date/time of appointment and connection information.

**Example messages:**
**Patient Email:**
**Subj Line:** Your VA Video Visit has been scheduled for Wed 07 Sept 2022 13:00 Mountain Standard Time CRM: 00000
This is a reminder of your Video Visit with a VA clinician on **Wed 07 Sept 2022 13:00 Mountain Standard Time**. Please click the following link to access the virtual meeting. This will take you into the virtual waiting room until your provider joins. [Click Here to Join the Virtual Meeting](#)

**Service Type:** Test Service

**Clinician:** Provider, VA;

If you have any questions or concerns, please contact your clinic.

A calendar appointment is attached to this email, you can open the attachment and save it to your calendar.

**Provider Email:**

**Subj Line:** Scheduled Telehealth Appointment Notification for Test Service to Home/Mobile Wed 07 Sept 2022 13:00 Mountain Standard Time CRM: 00000

This is an automated Message to notify you that a Telehealth Appointment has been Scheduled for Wed 07 Sept 2022 13:00 Mountain Standard Time. Please open the attachment and click "Save and Close" to add this event to your calendar. The Details are listed below:

**Provider Site Information:**

**Room:** Bldg. Mountain Towers, Room 817 @ Glendale, CO CBOC (554)

**Vista Clinic:** Provider Test Clinic @ Glendale, CO CBOC (554ZX)

**Technologies:**

CVT Web Cam / Software Client System: Camera.Test1 @ Glendale, CO CBOC (554ZX); POC Name: Specialist, Telehealth; POC Phone #: 555-123-4567

- Camera, Videoconferencing / Web

**Provider:** Provider, VA; Phone: 555-345-6789

**Provider Site Emergency Responsibilities:**

Provider will assure that s/he has a direct, fail-safe emergency contact phone number for the patient site and immediately call this number to notify patient site staff of the emergency. Provider will assure that s/he has police and/or 911 emergency numbers for the patient location. Provider will stay on the videoconferencing call to assist patient site staff during the emergency. Provider agrees to facilitate continued care/hospitalization for Veteran patient, if necessary. Note frequency of Telehealth provider or Surrogate log in to Patient Site CPRS to receive/view/respond notifications based on the site’s critical value policy.

**Telephone Contact Information:**

- To direct dial the room: 555-678-1111
- To contact the TCT at the provider site, call Telehealth Specialist at 555-123-4567.

**Home/Mobile Information:**

**Site DEA Licensed:**

This is a Home/Mobile visit, consider Ryan Haight regulations prior to prescribing any controlled medications.

**Virtual Meeting Space:**
From your Web browser:
https://care.va.gov/vvcapp/?name=Provider&join=1&media=&escalate=1&conference=VVC9001@care.va.gov&pin=0771785#

And if you wanted to dial from your VTC device:

From any VTC device: vvc9001@care.va.gov
Host CID: 0771785#

Please Do Not Reply to this message. It comes from an unmonitored mailbox.

This is currently what is in the body of the email for DALC Issued Tablet Patient and Provider Email Notifications.

Patient Email:
Subj Line: Your VA Video Visit has been scheduled for Thu 15 Sept 2022 13:00 Eastern Standard Time CRM:0377139

This is a reminder of your Video Visit with a VA clinician on Thu 15 Sept 2022 13:00 Eastern Standard Time. Your provider will call your CVT tablet for the appointment.

Service Type: Test Service
Clinician: Telehealth Specialist.

If you have any questions or concerns, please contact your clinic.

A calendar appointment is attached to this email, you can open the attachment and save it to your calendar.

Provider Email:
Subj Line: Scheduled Telehealth Appointment Notification for Test Service to Home/Mobile Thu 15 Sept 2022 11:00 Mountain Standard Time CRM:0377138

This is an automated Message to notify you that a Telehealth Appointment has been Scheduled for Thu 15 Sept 2022 11:00 Mountain Standard Time. Please open the attachment and click “Save and Close” to add this event to your calendar. The details are listed below:

Provider Site Information:
Room: Bldg. Mountain Towers, Room 817 @ Glendale, CO CBOC (554)
Vista Clinic: GLE TH PACT PC TEST NP PAT @ Glendale, CO CBOC (554)
Technologies:
CVT Web Cam / Software Client System: Test Camera1 @ Glendale, CO CBOC (554); POC
Name: Specialist, Telehealth

Provider: Specialist, Telehealth
**Provider Site Emergency Responsibilities:**
Provider will assure that s/he has a direct, fail-safe emergency contact phone number for the patient site and immediately call this number to notify patient site staff of the emergency. Provider will assure that s/he has police and/or 911 emergency numbers for the patient location. Provider will stay on the videoconferencing call to assist patient site staff during the emergency. Provider agrees to facilitate continued care/hospitalization for Veteran patient, if necessary. Note frequency of Telehealth provider or Surrogate log in to Patient Site CPRS to receive/view/respond notifications based on the site’s critical value policy.

**Telephone Contact Information:**
- To direct dial the room: 555-678-1111

**Home/Mobile Information:**

**Site DEA Licensed:**
This is a Home/Mobile visit, consider Ryan Haight regulations prior to prescribing any controlled medications.

Patient CVT Tablet: sip:SERIAL#bltablet@evn.va.gov

Please Do Not Reply to this message. It comes from an unmonitored mailbox.

Internally, the following information is used:
- Connection information for video appointments using GFE. This connection information is sent to the visit provider via internal VA Outlook Exchange e-mail. (See above examples)
- Veteran information (name presently, eventually last 4 SSN) appears in Views (screen reports or lists) of service activities/appointments as used by providers, schedulers, and clinic staff to identify a patient for an appointment/service activity for a specific kind of visit (clinic-based, home-based) and, if clinic-based, at which clinic site.
- If a clinic-based visit involves 2 different VistA systems, TMP uses the patient information to register the Veteran in both VistA systems to allow VistA appointments to be made in both systems to enable workload collection at both sites.
- The IP address of the patient site VA networked PC is retrieved from the TMP Technology record when that technology is scheduled to be used for patient care within TMP and is used within an e-mail invitation to the telehealth provider as below. The IP address is accessed by clicking the icon “invitation.cvl.” The provider PC is then connected to the patient site PC and the digital stethoscope is enabled for use.

**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

In general, the information stored in TMP is used to prepare various management, tracking, and follow-up reports that are used to assist in the management and operation of the healthcare facility, and the planning, scheduling, and delivery of patient medical care.

Microsoft CRM has internal tools to generate graphs and reports of specific data. At this time there are no printed reports using Veteran-specific data. All reporting is aggregated.

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?

- Transfers are protected by HTTPS using certificate exchange and SSL encryption. Role-based security with the TMP application to limit user access to PII and PHI information on systems.

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

- Patient MVIs are used in place of SSN. The TMP application does not retain any sensitive data.

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

- No sensitive information is retained. Role-based security within the TMP application limits user access to PII and PHI information. HTTPS using SSL encryption and Certificate exchange is used when data is transmitted. Mandatory annual training in areas of PII/PHI security, Data Privacy, and HIPAA.

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?
VBA ensures that the practices stated in the PIA are reinforced by requiring all applicable Contractors and VA employees to complete all the following VA training: VA Privacy and Information Security Awareness and Rules of Behavior Training, and Privacy and HIPAA-focused training. Contractors and VA employees are required to agree to all rules and regulations outlined in training, along with any consequences that may arise if failure to comply. Our facilities employ all security controls in the respective high-impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 and specific VA directives. VA Records Management Policy and the VA Rules of Behavior in the VA Talent Management System (TMS) govern how Veterans’ information is used, stored, and protected.

Customized Microsoft internal security roles are designed and employed to control all access to data stored within TMP.

**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*

Although the Department of Defense’s Electronic Data Interchange Personal Identifier (EDIPI) is requested in the Patient Search Screen, it is not retained within the system.

Visible within the TMP system patient record:
- Last 4 SSN
- Identity Theft Indicator
- Legal Name, First, Middle, and Last
- Legal Name Suffix
- Internet Protocol (IP)
- Other Names (Aliases)
- Email
- CVT Tablet connection information
- Tablet Type
- Phone number, mobile, home, and business
- Emergency contact information
- Provider Virtual Meeting Space URL (now obsolete, used for pilot)
- Patient Virtual Meeting Space URL (now obsolete, used for pilot)
- Home Address
- Home Country
- Time Zone
• Gender
• Marital Status
• Deceased indicator
• Date of Birth
• Branch of Service
• Deceased Date
• Identity Theft Indicator
• Integration Control Number (ICN)
• CORP, BRLS

Not visible within the TMP system patient record without specific security role:
• Identifier Type
• Identifier
• Assigning Facility
• Assigning Authority

Visible within the TMP system technology record:
• VA networked PC IP address for the patient site

Not visible within the e-mail invitation to use the digital stethoscope
• VA networked PC IP address for the patient site

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 a 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.

TMP records are retained and disposed of in accordance with the records disposition authority approved by the Archivist of the United States. Health information stored on electronic media is maintained for 75 years after the last episode of patient care and then deleted RCS 10-1 10 (https://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.

TMP records are retained and disposed of in accordance with the records disposition authority approved by the Archivist of the United States. When managing and maintaining VA data and records, healthcare facilities will follow the guidelines established in the NARA-approved Department of Veterans’ Affairs Record Control Schedule (RCS) 10-1 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf)

A Backup Plan and Restore Plan is developed and implemented for the computing environment using industry best practices. At a minimum, the plan shall include the requirement to save data for the backup and recovery of information stored on the cloud storage infrastructure to meet related Standard Level Agreements (SLAs) and the retention of records as required by VA Handbook 6300.1 (Records Management Procedures) and VA Directive 6300 (Records and Information Management).

CRM production data is retained for 14 days and restored to each application’s production environment per request. Backups are conducted daily and as needed per application team request.

The Federal Records Act of 1950, as amended, contains the statutory authority for VBA records management. Government-wide responsibility for Federal recordkeeping is shared by the General Services Administration (GSA) and NARA. Title 44 of the United States Code (U.S.C.) §§ 3301 through 3314 establishes the legal basis for the disposal of records of the United States Government. All electronic permanent records and VA sensitive information records are treated the same as hardcopy records and should follow an approved record disposition plan, see VBA RCS (VB-1)(VB-2), to include; (1) retaining, (2) transferring to a records center for temporary storage, (3) transferring to an archival agency, (4) donating to an eligible repository, and (5) transferring to an approved image reproduction vendor.

**NOTE:** Never delete permanent records or VA-sensitive information.

It is VBA policy that all Federal records contained on paper, electronic, or other media are properly managed from creation through final disposition, in accordance with federal laws, the General Records Schedule (GRS), and VBA Records Control Schedule (VBA RCS) (VB-1) (VB-2). VBA is committed to enforcing the proper disposition of Veterans’ records by ensuring the records are appropriately protected and maintained. The Records Management Officer (RMO), Records Management Technician (RMT), and supervisors will work together to ensure all VBA employees and affected parties follow.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:** Paper documents received are scanned into VA’s electronic document repository and subsequently destroyed after 90 days. Electronic records are not purged.
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

The TMP application follows NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process of any IT storage hardware used in the ECC application. The Guidelines establish three levels of data destruction: Clear, Purge, and Destroy, which can be applied to different data storage devices. An appropriate destruction method will be chosen based on the memory type (Flash Memory Magnetic Drives, Optical Devices, Hard Copies etc.) used for the storage. It is VA policy that all Federal records contained on paper, electronic, or other media are properly managed from their creation through their final disposition, in accordance with Federal laws, the General Records Schedule, and the VBA Records Control Schedule VBA RCS (VB-1) (VB-2). It provides a brief description of the records and states the retention period and disposition requirements. It also provides the NARA disposition authorities or the GRS authorities, whichever is appropriate for the records, in addition to program and service sections.

Regarding temporary paper records, in particular, those that contain PII, and VA sensitive information, which are under the jurisdiction of the VA, will be handled securely, economically, and effectively and disposed of properly. Written documentation that attests to the completion of the destruction process after the final destruction is required, which could be in the form of a letter, memo, or any format attesting to its complete destruction. This certification is not considered a valid certification of destruction if completed and submitted prior to the final destruction of the records. The certification should contain sufficient information to attest to the final destruction of the temporary paper records – what temporary records were destroyed, the date when they were destroyed, what destruction method was used, where they were destroyed, and who was responsible for their final destruction. (VA Directive 6371, 04/08/2014).

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

No PII is used for research or training purposes.

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.

**Privacy Risk:** There is a risk that the information maintained by TMP could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

**Mitigation:** To mitigate the risk posed by information retention, TMP adheres to the disposition authority approved by the Archivist of the United States. When the retention date is reached for a record, the individual’s information is carefully disposed of.

**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>Master Veterans Index (MVI)</td>
<td>To accomplish scheduling of healthcare delivery to Veterans</td>
<td>Veteran contact information Medical information Scheduled appointment information</td>
<td>Transfers are protected by HTTPS using certificates that identify both Partner and VLER DAS computers.</td>
</tr>
<tr>
<td>National Telehealth Technology Help Desk (NTTHD)</td>
<td>NTTHD provides tech support to TMP users and so may, on need to do so basis, access TMP service activity and technology screens. NTTHD also provides technical support for home based video calls and may receive calls from Veterans. We have confirmation that NTTHD is authorized for patient contact and to access patient information on a need-to-know basis.</td>
<td>In the case of VMR generation failures, NTTHD may need to access Patient Search/MVI information and/or application integration failure logs</td>
<td>TMP system screens</td>
</tr>
<tr>
<td>Veterans Health Administration</td>
<td>Integration of veteran PHI across healthcare facilities</td>
<td>Clinical data that may contain Protected Health Information (PHI) appropriate to the</td>
<td>HTTPS using SSL Encryption</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Program Office/IT System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veterans Relationship Management</td>
</tr>
<tr>
<td>HealthShare Integration and Data Access (HIDA)-Veterans Data Integration and Federation (VDIF)</td>
</tr>
</tbody>
</table>

Telehealth Appointments

Provides call center case tracking and legacy integration services to a national network of call centers

PII/PHI for Veterans for MVI Person Search and MVI Proxy Add to VistA via VRM VIMT; sent to / received from VRM

HTTPS using SSL encryption and Certificate exchange with VRM

To obtain broker services for translation and distribution of TMP HL7 Telehealth appointment messages to/from enterprise VistA Scheduling application databases

PII for Veteran patients and Telehealth clinicians required to schedule, update and cancel Telehealth appointments

HTTPS using SSL encryption

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.

Privacy Risk: The privacy risk associated with maintaining PII is that sharing data within the Department of Veterans Affairs could happen and that data may be disclosed to individuals who do not require access and heightening the threat of the information being misused. Risks are comparable to those associated with scheduling appointments in VISTA.

Mitigation: TMP strictly adheres to the principle of need-to-know. Only personnel with a clear business purpose are allowed access to the system and the information contained within. Again, mitigation is achieved by applying the same business rules for scheduling in VISTA to scheduling in TMP. Access to the VA networked PC IP addresses is controlled by CRM security roles and accessed on a need-to-know basis.

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 an 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

<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>None</td>
<td></td>
<td></td>
<td></td>
<td></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:** 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 the use 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 the 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.
The Notice of Privacy Practice (NOPP) is a document that explains the collection and use of protected information for individuals applying for VHA benefits. A signed statement acknowledging that the individual read and understood the NOPP is scanned into each applicant’s electronic file. When updates are made to the NOPP copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.

The Department of Veterans Affairs provides additional notice of this system by publishing one System of Record Notice (SORNs):

Specific to TMP, SORN 168VA005/86 FR 6975 was published in the Federal Register. It was printed in Vol. 86, No. 14 on Monday, January 25, 2021. Patients are also provided with privacy act statements on forms.

SORN 150VA19-E8-28183– Administrative Data Repository- VA

SORN 58 VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

Cloud usage and storage, SORN 173VA005OP2/86 FR 61852

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

Patients can refuse to provide information if they choose. There is no penalty for not providing the information.

Veterans have the right to refuse to disclose their SSNs to VBA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VBA an SSN (38 Code of Federal Regulations CFR 1.575(a)).

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

All requests 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 VBA address outlined within the SORN.
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?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

Privacy Risk: There is a risk that Veterans who provide information to the TMP application, as mentioned above, will not know how their information is being stored. If the information collected in TMP is inaccurate or outdated, it could cause an individual’s health information to be released to the incorrect party. If the notification e-mail carrying the IP address of the VA networked PC were to be misdirected or the e-mail “hacked,” unauthorized access to the VA network is possible.

Mitigation: This PIA serves to notify Veterans calling into the call center about the collection and storage of personal information. Individuals provide information directly to the VA Medical Center (VAMC) medical staff. Any validation performed would merely be the individual personally reviewing the information before they provide it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data.

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 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 may request access to Privacy Act records maintained by requesting a copy in writing. 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 VBA 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.

Access to and use of national administrative databases are limited to those persons whose official duties require such access, and the VA has established security procedures to ensure that access is appropriately limited. Information security officers and system data stewards review and authorize data access requests. VA regulates data access with security software that authenticates users and requires individually unique codes and passwords. VA provides information security training via VA TMS to all staff and instructs staff on the responsibility each person has for safeguarding data confidentiality. Members of the public are not allowed access to the TMP system. An individual who wishes to determine whether a record is being maintained under his or her name in the TMP system or wishes to determine the contents of such records should write the Director Standards and Interoperability Chief Health Informatics Office/Office of Informatics and Analytics/Veterans Health Information.

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.

All corrections to patient information are recorded by MVI; and then this system can pull the latest, up-to-date information regarding the patient record. Connection information is corrected by local telehealth clerical/scheduling staff within the TMP system.

Veterans have the right to amend their records by submitting their requests in writing. 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 VBA that maintains the record, in this case, the Director Standards and Interoperability Chief Health Informatics Office/Office of Informatics and
Analytics/Veterans Health Information. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VBA system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and 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.

If two sites failed to connect using the IP address contained within the e-mail notification for use of the digital stethoscope, the TMP Resource Manager for that patient site PC would be contacted directly to get accurate information for updating in TMP.

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 a 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.

Individuals are not notified if there is missing or inaccurate information in their records. An individual who wishes to determine whether a record is being maintained under his or her name in the TMP system or wishes to determine the contents of such records should write to the Director of Standards and Interoperability Chief Health Informatics Office/Office of Informatics and Analytics/Veterans Health Information. Veterans have the right to request amendment of erroneous information in accordance with the Privacy Act. Individuals have the right to request an amendment (or correction) to information in the TMP records if they believe it is incomplete, inaccurate, untimely, or unrelated to their healthcare. All amendment requests should be submitted to the facility Privacy Officer at the VBA facility that maintains your information. In response, the individual may do any of the following:

- File a “Statement of Disagreement”
- Ask that your initial request for amendment accompany all future disclosures of the disputed information.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. 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.

If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures in sections 7-3, and state that the documentation they are now providing supersedes those previously provided.
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 incorrect information is accidentally recorded in an individual’s record. An individual may want to review the content of their record to check for data accuracy.

**Mitigation:** An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifiers, or who wants to review the contents of such a record, should submit a written request or apply in person to the VBA facility where care was rendered. Inquiries should include the patient’s full name, SSN, and return address.

The health care facilities Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal 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 TMP is provided at two levels. Office of Information Technology (OIT) staff members hold programmer keys that permit full access. Local staff can set up local report parameters and run local reports. Annual training on VA Privacy and Information Security Awareness is tracked on the VA TMS. Microsoft CRM allows for security roles for access to different functions and data within the system according to the need for access. Role assignment is determined by function, individuals who do not perform a particular function are not assigned those security roles. Security roles are assigned by system administrators, and requests are submitted to NTTHD who forward them to system administrators. There is the chance that the completion of this PIA could potentially result in technology changes, so long as the changes are required by OIT and not simply suggested or discretion over implementation is given.

**Developer Access**

Developers’ account management processes should further ensure that only end-users are able to access the environment. Developers and ECC Project teams will work to create, update, access, and disable developer accounts for project teams. Additionally, there shall be a review of user access periodically to evaluate whether users are active in the environment; if the user is not active, their account is terminated. A designated VA Project POC is the only person who may submit account creation requests and submitted for accountability purposes.

**End-User and Tester Access**

All individuals requesting developer access are required to complete all VA training (VA Privacy and Information Security Awareness and Rules of Behavior Training, Privacy and HIPAA Focused Training, and Information Security for IT Specialists Training) and must be authorized by VA Project Manager. To ensure that this requirement is met, the designated VA Project POC must submit a signed Access Request Form for an individual or a group. At a minimum, the following information should be provided for each VA Project Team member requesting access to the ECC application Environments: First Name, Last Name, Primary Email, Main Phone, Manager, Current on VA Training, VA Employee or Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date.

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 Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed, and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please
describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

Yes, there are contract system administration personnel who maintain the server hardware and software but are not primary users of the TMP system itself. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Roles of Behavior training via the VA TMS.

As discussed above, NTTHD, as a contracted group, has access to the system and is authorized by system administrators to provide support and high-level data functions/entities.

All contractors with access to the system must go through a background check/investigation via the office of Personnel Management (OPM). All contractors accessing the environments must comply with all access and security requirements. Contractor access to the system expires at the end of the contract duration or earlier.

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.

Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA’s Talent Management System (TMS). After the TMP user’s initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training.

TMP users agree to comply with all terms and conditions of the National Rules of Behavior, by electronically signing the Rules of Behavior certificate of training after successfully completing the training session.

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.

1. Security Plan Status:
2. Security Plan Status Date:
3. Authorization Status:
4. Authorization Date: 6/10/2022
5. Authorization Termination Date: 12/07/2022
6. Risk Review Completion Date:
7. FIPS 199 classification of the system: The TMP System Security Impact is Moderate

VRM CRM Application Framework Access (TMP falls under this umbrella application) received full Authority to Operate on 6/10/22 with an expiration of 12/07/22.

Based on the FIPS 199 analysis, the TMP System Security Impact 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.

Yes, the following cloud hosting solutions are currently used:
- Government Community Cloud (MSFT D365 SAAS)

- Dynamics 365 Government is designed to support the Federal Risk and Authorization Management Program (FedRAMP) accreditation at a High-Impact level. FedRAMP artifacts are available for review by federal customers who are required to comply with FedRAMP. Federal agencies can review these artifacts in support of their review to grant an Authority to Operate (ATO).

- Dynamics 365 Government has features designed to support customers’ CJIS Policy requirements for law enforcement agencies. Visit the Dynamics 365 for Customer Engagement apps Trust Center for more detailed information related to certifications and accreditations.

- Government Azure Cloud

- Azure and Azure Government have earned a Provisional Authority to Operate (P-ATO) at the High Impact level from the Joint Authorization Board, the highest bar for FedRAMP accreditation. The Federal Risk and Authorization Management Program (FedRAMP) is an assessment and authorization process for cloud service providers (CSPs). Specifically, the process is for CSPs that create cloud solution offerings (CSOs) for use with federal agencies.

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.*

Per Azure Customer Data Protection Policy ([https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data](https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data)), Microsoft does not inspect, approve, or monitor applications that customers deploy to Azure. Moreover, Microsoft does not know what kind of data customers choose to store in Azure. Microsoft does not claim data ownership over the customer information that’s entered into Azure.

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.*
Per the Azure Data Usage Policy (https://docs.microsoft.com/en-us/azure/cyclecloud/data-policy?view=cyclecloud-8), the Azure CycleCloud tool collects anonymized usage data by default and sends this telemetry data to Microsoft. Microsoft may use this data to understand how users interact with CycleCloud to support and improve the CycleCloud product. The data is anonymized and does not include any personally or organizationally identifying data. The collected data is governed by the Microsoft Privacy Policy.

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.

Azure and Azure Government have earned a provisional authority to operate (P-ATO) at the NIST SP 800-53 High Impact level from the Joint Authorization Board. This level represents the highest bar for FedRAMP accreditation, and it authorizes the use of Azure and Azure Government to process highly sensitive data.

These Azure and Azure Government certifications satisfy the security controls, privacy controls, and records retention policy requirements for AAL1, AAL2, and AAL3.

The FedRAMP audit of Azure and Azure Government included the information security management system that encompasses infrastructure, development, operations, management and support of in-scope services. When a P-ATO is granted, a cloud service provider still requires authorization (an ATO) from any government agency it works with. For Azure, a government agency, or organizations working with them, can use the Azure P-ATO in its own security authorization process. The agency or organization can rely on it as the basis for issuing an agency ATO that also meets FedRAMP requirements.

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).

Robotics Process Automation is not utilized
## 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>ID</td>
<td>Privacy Controls</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>UL</td>
<td>Use Limitation</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 they provided in this Privacy Impact Assessment is true and accurate.

Jacquelyn R Filkins 190940
Date: 2022.10.12 16:33:26 -04'00'

Privacy Officer, Jacquelyn R Filkins

Thomas J. Orler 178546
Date: 2022.10.14 07:28:02 -05'00'

Information System Security Officer, Thomas J Orler

Stefano Masi 474380
Date: 2022.10.19 07:48:11 -04'00'

Information System Owner, Stefano Masi
APPENDIX A-6.1

The Information Bulletin (IB) 10-163, Notice of Privacy Practices can be found at the following website:


SORN (https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf)

Federal Register Vol 73 (E8-28183.pdf (govinfo.gov))

Citation of the legal authority to operate the IT system is “Title 38, United States Code, Section 501 – Veterans’ Benefits” and “SORN 58 VA21/22/28, 38 USC 1781, 1802, 1724, 1728, 1703, 1725, 1728, 1781, 1803 and Public Law 103-446 section 107”.

Administrative Data Repository SORN, 150VA19-E8-28183

Cloud usage and storage, SORN 173VA005OP2/86 FR 61852

Health Information Exchange, SORN 168VA10P2
