Privacy Impact Assessment for the VA IT System called:

Telehealth Management Platform (TMP)

Veterans Affairs Central Office (VACO)

Software Product Management (SPM)

eMASS ID #2292

Date PIA submitted for review:

2/12/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dennis Lahl	dennis.lahl@va.gov	202-461-7330
Information System Security Officer (ISSO)	Thomas Orler and Albert Estacio	Thomas.Orler@va.gov and Albert.Estacio@va.gov	708 938-1247 and 909 583-6309
Information System Owner	Laura Young	Laura.Young3@va.gov	847-420-7401

Abstract

The abstract provides the simplest explanation for "what does the system do?".

Telehealth Management Platform (TMP) provides on-demand access to comprehensive VA services and benefits in a consistent, user-centric manner through a multi-channel virtual call center (VCC) processing framework.

Overview

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

1 General Description

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

IT system name: Telehealth Management Platform (TMP)
Program Office: Software Product Management (SPM).

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

TMP provides a national patient appointment scheduling system to support Clinical Video Telehealth (CVT), workload capture/identification, and reservation of resources. TMP ensures resources (health care providers, locations, and equipment) are reserved for patient appointments by coordinating with disparate Veterans Health Information Systems and Technology Architecture (VistA) systems and the Cerner System.

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

VA Owned and VA Operated.

2. Information Collection and Sharing

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

TMP currently has data on over five million veterans who have had Telehealth appointments scheduled through TMP.

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

TMP collects and processes PII/PHI and network security records to assist in processing care for Veterans and Beneficiaries.

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

TMP provides VHA clinical schedulers and providers with a single interface to manage Telehealth appointments, health care 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 Personal Identification Numbers (PINs) for one-touch video connectivity. The TMP software has bi-directional secure interfaces to the VA Veterans Information System and Technology Architecture (VistA) 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 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.

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

TMP has a single instance in the Production environment; therefore, it is not operated in more than one site.

3. Legal Authority and SORN

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

Title 38 U.S. Code § Section 513, Title 38, United States Code, Section 501 – Veterans' Benefits" and "38 USC 1781, 1802, 1724, 1728, 1703, 1725, 1728, 1781, 1803 and Public Law 103-446 section 107.

SORNS:

(1) 58VA21/22/28 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA" (11/8/2021) https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf
(2) 57VA10B2A, Voluntary Service Records-VA (8/29/2016) https://www.govinfo.gov/content/pkg/FR-2016-08-29/pdf/2016-20606.pdf
(3) 150VA19, Administrative Data Repository-VA (11/26/2008) https://www.govinfo.gov/content/pkg/FR-2008-11-26/pdf/E8-28183.pdf
(4) 79VA10/85FR84114, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf
(5) 24VA10A7, Patient Medical Records-VA (10/02/2020) https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf
(6) 168VA005, Privacy Act of 1974; System of Records (01/25/2021) Federal Register :: Privacy Act of 1974; System of Records

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

The SORN does not require amendment, revision, or approval. Additionally, the SORN covers cloud usage.

4. System Changes

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

Completion of the PIA will not require changes in the business process.

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

Completion of the PIA will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]

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

☐ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements:

Additional SPI Collected:

- Patient demographics
- Patient unique person identifiers (Patient Integration Control Number, Patient Data File Number)
- Patient appointment information
- Integration results
- Clinical Data
- Veteran medical information

PII Mapping of Components (Servers/Database)

TMP consists of one key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by TMP and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Telehealth Management Platform (TMP) Application	**Yes**	**Yes**	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number(s), Personal Fax	PII is collected and stored so that TMP can verify the identity of the Veteran. , Clinical Data and Veteran medical	This application is within VA and has FIPS 2.0 encryption.

			Number, Personal Email Address, Emergency Contact Information, Patient demographics, Patient unique person identifiers (Patient Integration Control Number, Patient Data File Number), Patient appointment information, Integration results, Clinical Data that may contain Protected Health Information (PHI) appropriate to the Telehealth Appointments, Veteran medical information	information is stored to describe the reason for the appointment.	
MVI (Master Veteran Index)	**Yes**	**Yes**	Patient ICN (Integration Control Number), DFN (Data File Number)	PII is stored to uniquely identify the Veteran.	This application is within VA and has FIPS 2.0 encryption.
VistA	**Yes**	**Yes**	Name, Email address, ICN, DFN	PII is stored to uniquely identify the Veteran	This application is within VA and has

					FIPS 2.0 encryption.

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

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

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

Information is from the Master Veterans Index (MVI) system, based on a search of the MVI.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

TMP provides a national scheduling system to support Clinical Video Telehealth (CVT). TMP queries the MVI system to positively identify a Veteran.

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

TMP runs reports on workload and interactions.

1.3 How is the information collected?

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

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

TMP queries the MVI system to positively identify a Veteran.

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

The information is not collected on a form and is not subject to the Paperwork Reduction Act.

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

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

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

Information regarding veterans and providers in TMP is almost entirely sourced and synced from authoritative systems within VA for that data (VistA, MVI, etc.). Most of this data contains Globally Unique Identifiers (GUIDs) which, if corrupted, will prevent actions being taken on the authoritative systems (appointments in VistA, Cerner, Video Visit Service.

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

No commercial aggregator is used.

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

Title 38, United States Code, Section 501-Veterans' Benefits, Joint Commission National Patient Safety Goals- Goal 1: Improve the accuracy of patient identification, The Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a), Executive Order 9397. Title 38 U.S. Code § Section 513, Title 38, United States Code, Sections 501(b) and 304.

SORNS:

(1) 58VA21/22/28 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA" (11/8/2021) https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf
(2) 57VA10B2A, Voluntary Service Records-VA (8/29/2016) https://www.govinfo.gov/content/pkg/FR-2016-08-29/pdf/2016-20606.pdf
(3) 24VA10A7, Patient Medical Records-VA (10/02/2020) https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:

Where TMP collects Personally Identifiable Information (PII), if this information were released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to those individuals.

Mitigation:

Applications mitigate the risk of identity theft by requiring all applicable Contractors and VA employees who engage with TMP to complete all the following data security and privacy VA trainings:

- VA Privacy and Information Security Awareness and Rules of Behavior Training
- Privacy and HIPAA focused training

Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply.

TMP 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 National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 and specific VA directives.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Veteran's identification	Not used
Social Security Number	Used to verify Veteran identity	Not used
Date of Birth	Used to verify Veteran identity	Not used
Personal Mailing address	Used to correspond with Veteran	Not used
Personal Phone Number(s)	Used to correspond with Veteran	Not used
Personal Fax Number	Used to correspond with Veteran	Not used
Personal Email Address	Used to correspond with Veteran	Not used
Emergency Contact Information (Name, Phone Number, etc. of a different individual)	Used in emergencies to contact the Veteran	Not used
Internet Protocol (IP) Address Numbers	Used to interface with Telehealth equipment used during the clinical appointment	Not used
Patient demographics	Used to verify Veteran identity	Not used
Patient unique person identifiers (Patient Integration Control Number, Patient Data File Number)	Used to verify Veteran identity	Not used
Patient appointment information	Used to schedule an appointment for the Veteran	Not used
Integration results	Used to confirm the appointment was scheduled for the Veteran	Not used
Clinical Data	Used to schedule appointment for the Veteran	Not used
Veteran medical information	Used to schedule appointment for the Veteran	Not used

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

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

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 health care facility, and the planning, scheduling, and delivery of patient medical care. Microsoft CRM has internal tools to generate graphs and reports of specific data. Currently there are no printed reports using Veteran-specific data. All reporting is aggregated.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for *the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.*

TMP does not create new information.

2.3 How is the information in the system secured?

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

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

Data within the VA network is FIPS 2.0 encrypted.

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

For TMP, specifically, in lower environments, test records are used. In production, Telehealth Schedulers, and Scheduling Managers are the only users with permission to view SSN when scheduling patient visits in VistA for Telehealth providers. All other application users are blocked from accessing SSN. VEIS uses HTTPS, TLS, oAuth tokens and OSP APIM for additional encryption.

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

Contractors and VA employees are required to take Privacy, HIPAA, and information security training annually. HTTPS using SSL encryption is used between internal VA systems. Personnel accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. VEIS uses HTTPS, TLS, oAuth tokens and OSP APIM for additional encryption.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

VA ensures that the practices stated in the PIA are reinforced by requiring all applicable Contractors and VA employees to complete all the following VA trainings: 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 trainings, 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 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.

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

Yes, criteria, procedures, controls, and responsibilities are documented.

2.4c Does access require manager approval?

Yes, access requires manager approval.

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

Yes, it is the responsibility of the project making the request to ensure compliance with VA regulations and policies regarding configurations, privacy restrictions, network access and authorities or operates. (Including but not limited to: VA 6500, TIC, PIA/PTAs, SORN, and application ATOs).

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

It is the responsibility of the project making the request to ensure compliance with VA regulations and policies regarding configurations, privacy restrictions, network access and authorities or operates (including but not limited to: VA 6500, TIC, PIA/PTAs, SORN, and application ATOs).

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:

- SSN
- Identity Theft Indicator
- Legal First Name
- Legal Middle Name
- Legal Last Name
- Legal Name Suffix
- Salutation
- Other Names (Aliases)
- Email
- CVT Tablet connection information
- Tablet Type
- Home Phone
- Mobile Phone
- Business Phone
- Provider Virtual Meeting Space URL (now obsolete, used for pilot)
- Patient Virtual Meeting Space URL (now obsolete, used for pilot)
- Home Street Address
- Home City
- Home State
- Home Zip Code
- Home Country
- Time Zone
- Gender
- Marital Status
- Deceased indicator
- Date of Birth
- Branch of Service
- Deceased Date
- Identity Theft Indicator
- Patient appointment information

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 Telehealth equipment
- Audit History for each transaction performed on each field
- Integration Results
- TMP User information
    - Business Phone Number
    - Email Address
    - Location Address

- Job Title

Unique Person Identifiers

3.2 How long is information retained?

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

Depending on the type of information being retained, the timeframe could range anywhere from 9 months to 75 years. For more specifics refer to table 3.3b below. Information is retained according to the disposition instructions documented in Records Control Schedule: VHA RCS 10-1 10 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf). Please refer to table 3.3b for each records retention schedule.

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

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

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

Yes, all records stored within the system of record are indicated on an approved disposition authority:

(1) Records Control Schedule (RCS) 10-1 The link to the RCS is as follows: https://www.va.gov/vhapublications/rcs10/rcs10.1.pdf
(2) OI&T RCS 005-1
(3) RCS VBA-1

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

Record	Record Control Schedule 10-1 Chapter	Record Control Schedule 10-1 Item Number	Disposition Instructions	Disposition Authority	Justification
Patient PII and Demographics, unique person identifiers	6000	6000.2	Destroy/delete 75 years after the last episode of patient care; however, some data may be moved to offline storage to alleviate the performance issues the application experiences when the database size reaches 10TB.	N1-15-02-3, item 3	Information is collected from the Master Veterans Index (MVI) system, based on a search of the MVI. TMP is not the source of truth, MVI is the source of truth
Patient appointment information	6000	6000.2	Destroy/delete 75 years after the last episode of patient care; however, some data may be moved to offline storage to alleviate the performance issues the application experiences when the database size reaches 10TB.	N1-15-02-3, item 3	TMP interfaces with VistA/Cerner, which is the official source of truth for patient appointment information. Scheduler inputs the Patient appointment information. TMP creates the appointment in other systems (VistA, Cerner, VVS). TMP keeps records that those appointments exist (pointers to those appointments).
Integration Results	2201 - Transitory and Intermediary Records	2201.1 Transitory Records	Destroy when no longer needed for business use, or according to agency predetermined time period or business rule. The business has decided that these records can be deleted 9 months after creation.	GRS 5.1, item 010, DAA-GRS 2017-0003-0001	This data is transitory in nature. These are just records of what happened when an integration was used. Basically, logs.
TMP User information (phone number, email, location address, job title, unique person identifiers)	2100-Information Systems Security Records	2100.3.b - System Access Records	Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use	DAA-GRS 2013-0006-0004, item 31	The user is a clinical scheduler or provider, not the Veteran.
Audit History	2000-General Technology Management Records	2000.2	Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.	DAA-GRS2013-0005-0004, item 020	Audit logs are growing exponentially, as it tracks all the actions performed on records by the users. In Production, All TMP tables have auditing enabled and it captures similar information for each field and who performed the CRUD (Create/Read/Update/Delete) operations on those fields.

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

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

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 application. The Guidelines establish three levels of data destruction: Clear, Purge, and Destroy, that 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 medium 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.

TMP is configured to automatically purge Audit History logs that are older than 3 years. This is necessary since the size of audit logs grows exponentially, as they track all actions (create/read/update/delete) performed on each field by each user.

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

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

No PII is used for research or training purposes. No real data is used for research, testing, or training.

<u>3.6 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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk:

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

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***
Master Veterans Index (MVI)	To identify the veteran.	Veteran contact information Medical information Scheduled appointment information	HTTPS using certificates that identify both Partner and VLER DAS computers.
Office of Community Care Help Desk (OCCHD)	To troubleshoot VMR generation failures, to provide tech support to TMP users, to provide tech support for home based video calls to Veterans.	In the case of VMR generation failures, OCCHD may need to access Patient Search/MVI information and/or application integration failure logs. OCCHD provides tech support to TMP users and so may, on need to do so basis, access TMP service activity and technology screens. OCCHD also provides technical support for home based video calls and may receive calls from Veterans. We have confirmation that OCCHD is authorized for patient contact and to access patient information on a need-to-know basis	Role-based TMP system screens, least privileged access. HTTPS using SSL
Veterans Health Administration	Clinical data	Clinical data that may contain Protected Health Information (PHI)	HTTPS using SSL
Veterans Relationship Management	To identify the veteran	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
HealthShare Integration and Data Access (HIDA)-Veterans Data Integration and Federation (VDIF)	To schedule or cancel clinical appointments.	Patient ICN	HTTPS using SSL encryption
VEIS (Veteran Experience Integration Solution)	To schedule or cancel clinical appointments.	Scheduled appointment Information, Patient ICN, Patient Contact Information, Patient Identification Information	HTTPS using SSL encryption and Certificate exchange with the VEIS App

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***
			services hosted on Microsoft Azure

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

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

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

Follow the format below:

<u>Privacy Risk:</u>

The privacy risk associated with 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 heightens the threat of the information being misused. Risks are comparable to those associated with scheduling appointments in VISTA.

<u>Mitigation:</u>

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 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***

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk:

TMP does no external sharing or disclosure.

Mitigation:

TMP does no external sharing or disclosure.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on an annual basis.

Privacy Policy: SORN 168VA005 was published in the Federal Register. It was printed in Vol. 77, No. 92 on Friday, May 11, 2012

SORN 24VA10A7 – Patient Medical Records - VA (https://www.oprm.va.gov/privacy/systems_of_records.aspx)

SORN Federal Register (FR) Link: Federal Register: Federal Register Citation

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to 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 was published in the Federal Register. It was printed in Vol. 77, No. 92 on Friday, May 11, 2012. Patients are also provided with a privacy act statement on forms.

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

The U.S. Department of Veterans Affairs, Veterans Health Administration, Notice of Privacy Practices can be found at this link: Notice_of_Privacy_Practices_VA_Poster_10-163.pdf

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

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A signed statement acknowledging that they 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 was published in the Federal Register. It was printed in Vol. 77, No. 92 on Friday, May 11, 2012. Patients are also provided with a privacy act statement on forms.

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.

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 (please refer to the 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.

VA permits individuals to agree to the collection of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VA Notice of Privacy Practices and conversations with VA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required. Where legally required VHA obtains signed, written authorizations from individuals prior to releasing, disclosing, or sharing PII and PHI. Individuals have a right to restrict the disclosure and use of their health information.

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

<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:

<u>Privacy Risk:</u>

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.

<u>Mitigation:</u>

This PIA and the Privacy Threshold Analysis (PTA) documents are privacy compliance and risk management assessment tools designed to document the collection, creation, maintenance, use and disclosure of personally identifiable information (PII) and personal health information (PHI) within an information technology (IT) system, program, rulemaking, or project. Both documents are available to the public and serve to notify Veterans calling into the call center about the collection and storage of personal information.

Section 7. Access, Redress, and Correction

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

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

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

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

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 Version Date: January 2020Page 17 of 23VBA 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.

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

The system is not exempt from the access provisions of the Privacy Act.

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

The system is a Privacy Act system.

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.

(1) All corrections to patient information are recorded by MVI. TMP pulls the latest, up-to-date information regarding the patient record from MVI.

(2) Connection information is corrected by local Telehealth clerical/scheduling staff within the TMP system.

(3) Veterans have the right to amend their records by submitting their request 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.

(4) If two sites fail 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 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.

Agents will notify the callers that they may change their information if the information presented is incorrect. VHA Handbook 1605.1, Appendix D: Privacy and Release Information, Section 8 states the rights of Beneficiaries to amend their records by submitting VA Form 10-5345a, Individual's Request for a Copy of Version Date: October 1, 2017, Page 18 of 25Their Own Health Information, that may be used as the written request requirement. This includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. System of Records

Notices provide a system Point of Contact. This PIA provides system owner to facilitate records correction.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Agents will notify the callers that they may change their information if the information presented is incorrect. VHA Handbook 1605.1, Appendix D: Privacy and Release Information, Section 8 states the rights of Beneficiaries to amend their records by submitting VA Form 10-5345a, Individual's Request for a Copy of Version Date: October 1, 2017, Page 18 of 25 Their Own Health Information, that may be used as the written request requirement. This includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. System of Records Notices provide a system Point of Contact. This PIA provides system owner to facilitate records correction.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

<u>Privacy Risk:</u>

There is a risk that individuals whose records contain incorrect information may not obtain access to TMP.

<u>Mitigation:</u>

TMP project staff would work with the affected individual and assist with opening an OIT Snow ticket for the individual.

Section 8. Technical Access and Security

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

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

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

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

For all roles, 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 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, requests are submitted to the VHA Office of Connected Care Help Desk (OCCHD)who forward the requests to system administrators.

Account management processes ensure that only end-users can access the environment.

Developers and ECC Project teams work to create, update, access and disable developer accounts for project teams. Additionally, quarterly reviews evaluate whether users are active in the environment; if the user is not active, their account is disabled.

A designated VA Project POC is the only person who may submit account creation requests for accountability purposes. 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 of individuals. At a minimum, the following information should be provided for each VA Project Team member requesting access to the application: 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.

All individuals requesting developer access are required to complete all VA trainings (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 receive authorization from a VA Project Manager.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Other agencies do not have access to TMP.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

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.

For all roles, 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 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, requests are submitted to the VHA Office of Connected Care Help Desk (OCCHD)who forward the requests to system administrators.

Account management processes ensure that only end-users can access the environment.

Developers and ECC Project teams work to create, update, access and disable developer accounts for project teams. Additionally, quarterly reviews evaluate whether users are active in the environment; if the user is not active, their account is disabled.

A designated VA Project POC is the only person who may submit account creation requests for accountability purposes. 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 of individuals. At a minimum, the following information should be provided for each VA Project Team member requesting access to the application: 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.

All individuals requesting developer access are required to complete all VA trainings (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 receive authorization from a VA Project Manager.

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

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

Yes, 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, OCCHD, 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 Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re-affirm 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. This training includes, but is not limited to, the following TMS Courses:

- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics

Role-based Training Includes but is not limited to and based on the role of the user.

- VA 1016925: Information Assurance for Software Developers IT Software Developers
- VA 3193: Information Security for CIOs Executives, Senior Managers, CIOs and CFOs
- VA 1357084: Information Security Role-Based Training for Data Managers

- VA 64899: Information Security Role-Based Training for IT Project Managers
- VA 3197: Information Security Role-Based Training for IT Specialists
- VA 1357083: Information Security Role-Based Training for Network Administrators
- VA 1357076: Information Security Role-Based Training for System Administrators
  VA 3867207: Information Security Role-Based Training for System Owners

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 02/20/2024
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 11/03/2023
5. *The Authorization Termination Date:* 05/01/2024
6. *The Risk Review Completion Date:* 10/31/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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

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

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes, TMP is a Software as a Service (SaaS). All VA Microsoft Dynamics 365 CRM applications are hosted in Microsoft Azure Government (MAG) cloud environment. Agreement with VA for service is through the VA Enterprise Cloud (VAEC) Azure – Service # -SR-001388.

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

<<ADD ANSWER HERE>>

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.

<<ADD ANSWER HERE>>

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.

<<ADD ANSWER HERE>>

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).

<<ADD ANSWER HERE>>

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**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2024.05.01 12:57:37 -04'00'

Privacy Officer, Dennis Lahl

THOMAS ORLER Digitally signed by THOMAS ORLER
Date: 2024.05.01 07:03:55 -05'00'

Information Systems Security Officer, Thomas Orler and Albert Estacio

LAURA YOUNG Digitally signed by LAURA YOUNG
Date: 2024.04.30 15:26:27 -05'00'

Information Systems Owner, Laura Young

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

The U.S. Department of Veterans Affairs, Veterans Health Administration, Notice of Privacy Practices can be found at this link: Notice_of_Privacy_Practices_VA_Poster_10-163.pdf

Privacy Policy: SORN 168VA005 was published in the Federal Register. It was printed in Vol. 77, No. 92 on Friday, May 11, 2012

SORN 24VA10A7 – Patient Medical Records - VA
(https://www.oprm.va.gov/privacy/systems_of_records.aspx)

SORN Federal Register (FR) Link: Federal Register: Federal Register Citation

HELPFUL LINKS:

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

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

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

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

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