Privacy Impact Assessment for the VA IT System called:

Telecare Record Manager Plus (TRM+)

Veterans' Health Administration (VHA)

Enterprise Program Management Office (EPMO)

eMASS ID # 1263

Date PIA submitted for review:

May 16, 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)	Roland Parten	Roland.Parten@va.gov	205-534-6179
Information System Owner	Tony Sines	Tony.Sines@va.gov	316-249-8510

Abstract

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

Telecare Record Manager Plus (TRM+) provides clinical call agents view-only access to information in VistA and CPRS including available in CPRS. It also provides the ability to generate TRM Plus notes and reports. The clinical call agent accesses protocols that guide assessment and documentation about the Veteran as well as previous encounters by selecting TEDP within TRM Plus. TEDP auto generates a note about the call as the clinical call agent selects patient responses to specific questions; it is used to document patient education as well as additional patient-specific documentation. TEDP Plus also selects the appropriate International Classification of Diseases Tenth Revision Clinical Modification (ICD-10 CM) and Current Procedural Terminology (CPT) codes. The output of clinical call agent's phone interactions process are progress notes in TRM Plus and CPRS that are automatically generated when signed by the clinical call agent. TRM Plus ensures the clinical call agent workload is captured. Some features of TRM Plus are summarized in the following: Telehealth encounters are becoming the industry normal to handle a multitude of patient issues. The use of this product enabled the Department of Veterans Affairs Health Administration to meet this need. TRM Plus capture numerous patient data objects during a single encounter. I.e., medications, evidence of flags in patient records, determination of which health condition to best focus on for a patient. Call Center agents interact with a patient to get refills of medications or referrals to Pharmacists. Specific medical information related to the call. Consistent flow of encounter to a referral agency or consults are completed. Consistent patient records documentation and proof of treatment for an encounter. Consistent documentation of any changes, modifications or accuracy of a patient records are completed.

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 is Telecare Record Manager Plus (TRM+), and it is owned by Enterprise Program Management Office

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

The business process is to ensure veterans who utilize telephone access can be greeted and triaged on issues related to their health care.

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

Richard Marble is the Information System Owner

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?*

Normal patient count can be between 250 – 400 calls per 8-hour shift. All Registered and Non-Registered Veterans.

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

The TRM Plus server is a single server that has executables set-up to handles all sites with licensing for the VISN. There are multiple executables short-cuts for the VistA connection to be made to and from.

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

Information sharing is not conducted on this server. This is completed by a Biometric report that is run off the SQL database.

The IT system has the TRM Plus application and Call Log Reporter on a Windows application server. The primary executables are launched from this server. The local workstation does interface with VistA to ensure that authentication of the user is maintained and managed.

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?*

TRM+ is only hosted at licensed VHA locations. The software requires a VistA account with approved role-based menus.

3. Legal Authority and SORN

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

TRM+ legal authorities for operating the system are found in the SORNS that apply to the particular component or minor system:

Veterans' Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).
Patient Medical Record – VA, SORN 24VA10A7 https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

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?*

These systems are not in the process of being modified nor is it using cloud technology.

4. System Changes

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

No changes are required.

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

No changes are required.

.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Record Number
☒ 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: Place of birth, System log files, Sample Clinical Data, clinical information related to the call.

PII Mapping of Components (Servers/Database)

TRM+ does not have any components mapped outside of VistA.

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
Telecare Record Manager Plus	Yes	Yes	Triage symptoms as reported by patient. Patient information is documents only in VistA Progress Note.	Ensure the right person is on the call, and the correct records is retrieved from VistA.	Data is encrypted

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

Veterans Health Administration - VistA	**yes**	**yes**	System Log Files, sample clinical data that may include Protected Health Information (PHI) Person full name (first, middle, and last) Social Security Number Date of birth Personal Mailing Address Telephone number Medical Record Number Emergency Contact Information Current Medications Race/Ethnicity	Electronically pulled from VistA through Computerized Patient record System (CPRS)	**Data is encrypted**

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?

TRM+ sources of information are reported via telephone interview. Other sources of data come from VistA Electronic Health Record, VistA Capri, and VBA documented information in Electronic Health Record.

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.

A normal medical review is not conducted such as vitals, Global Assessment Functioning (GAF) or Minnesota Multiphasic Personality Inventory (MMPI). Therefore, this type of patient cannot be physical reviewed. However, use of a mini mental exam, and certain question scripts have been done to assess these areas.

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

TRM+ integrates with both Veterans Health Information Systems and Technology Architecture (VistA) and Computerized Patient Record System (CPRS), and once integrated automatically creates a Text Integration Utilities (TIU) note in CPRS. TRM+ allows users to manage workload reporting, access patient information directly from VistA packages, access multiple VistA systems in the network, and access call history reporting for Completed, Pending, and Open Calls.

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?

The Patient/Veteran is asked questions over the phone during a patient telephone interview. No information is kept, but the information is gathered from this telephone interview from the questions are Person full name (first, middle, and last), Social Security Number, Date and place of birth, address, telephone number, etc. Then from the information given during the interview the review of data is then extracted from VistA Electronic Health Record, VistA CAPRI and VBA documents in the Electronic Health Record.

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?

TRM+ 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.

Verification is done monthly for accuracy performed by the site nurse managers/call center supervisors. Progress Notes, TIU notes and Call logs are all checked for accuracy.

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?

Hourly data checks are completed via VistA mirroring. The TRM Plus Server has a persistent report that monitors pre-determined threshold of services ran and completed.

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

Veterans' Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

Patient Medical Record – VA, SORN 24VA10A7 https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

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.

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The TRM Plus application retrieves and reviews Personally Identifiable Information (PII), Protected Health Information (PHI), and other highly delicate Sensitive Personal Information (SPI). If this information were to be 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. All strategies to ensure secure telephone transmissions are taken by each TRM Plus end user. This is done via the physical phone lines they use at a medical facility. Each record is reviewed by the Call Center Manager daily and weekly. Discrepancies are reported and corrected with the type of correction and strategies to counter them.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the Veteran in crisis, identify the potential issues and concerns, and offer assistance to the Veteran so that they may find the help they need to get through their crisis. By only reviewing the minimum necessary information, the VA is able to better protect the Veterans' information. Users are trained on how to handle sensitive information by taking VA Privacy and security awareness training and reading and attesting they understand the VA Rules of Behavior on an annual basis.

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.

All data collected or documented is placed into the patient Electronic Health Record. It is maintained for the life of the health record in VistA. In supporting proper medical triage at a telephone interactive point. Each triage encounter is screened during medical records committee reviews.

PII/PHI Data Element	Internal Use	External Use
Person full name (first, middle, and last)	Used as a veteran's identifier	Not used

Social Security Number	Assists in uniquely identifying the veteran's medical record	Not used
Date of Birth	Assists to identify age and confirm identity.	Not used
Personal Mailing Address	Used to contact veteran	Not used
Personal Phone Number	Used to contact veteran	Not used
Place of Birth	Used to confirm eligibility	Not used
Emergency Contact Information	Emergency use only	Not used
Medications	Used for refilling medications	Not used
Race/Ethnicity	statistical use	Not used
Medical Record Number	Used to identify veteran	Not used
Address	Used to contact veteran	Not used
Telephone Number	Used to contact veteran	Not used
System Log Files	Troubleshooting Application	Not used
Sample Clinical Data	Statistical use	Not used
Veteran's Service Connection	Medical treatment	Not used
Specific Clinical Information related to the call/visit	Medical treatment	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?

For all records that are developed concerning a patient they are reviewed by the local Medical Facility -Medical Records Committee. The Telehealth record is reviewed and audited using this same process and procedure. These records are reviewed weekly to monthly as prescribed in the Joint Commission Accreditation standards. For IT systems, the VistA system undergoes a consistent, constant, and predefined data review each day. Mirroring and authenticated storage are completed by the VA OI&T Office of Information Security.

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.

TRM+ does not analyze or produce patient data. The TRM+ application requires application-specific VistA menu option(s) and/or VistA security key(s) to retrieve, create, and store data in VistA.

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 is encrypted when it resides in VistA. Social Security Numbers are often abbreviated to give added protection. The hard drives that the applications/databases are hosted on are encrypted. Applications require specific menus/keys in VistA to access the inform.

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

Application protection: Only available to approved users, some applications use Patient Identifiers (PID) randomly generated within the application, some applications view SSNs in partial form, and/or application databases are encrypted.

VistA protection: Sensitive patient record tracking, only available to approved users via menus and keys, VistA Database, IRIS, is encrypted. SSN are viewable in partial for

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

> Application protection: Only available to approved users, some applications use Patient Identifiers (PID) randomly generated within the application, some applications view SSNs in partial form, and/or application databases are encrypted.
>
> VistA protection: Sensitive patient record tracking, only available to approved users via menus and keys, VistA Database, IRIS, is encrypted. SSN are viewable in partial form.

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?

PII access is followed by a Service Administrative Officer/Supervisor/designee(s) submit an ePAS request for new user's Veterans Health Information Systems and Technology Architecture (VistA) ePAS request can include VistA menu options/security keys, Clinical Patient Record System (CPRS) access, etc. The local VHA site OI&T is responsible to complete the ePAS request.

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

Organizational and Non-Organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly and VA Privacy and HIPAA training.

2.4c Does access require manager approval?

VHA facilities ISSO is responsibility to monitor VistA access and verify the TMS training has been completed and current. Careful attention to the Electronic Medical Record document process is followed and utilized by the recorder. Unauthorized person(s) are not allowed into this system.

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

Agent and the caller must assume responsibility to not discuss what is outside of the needed items for proper documentation. So, the same definition of how a medical provider handles sensitive information is the same an agent will adhere to.

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

All VHA staff are responsible for assuring safeguards for the PII.

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

Records related to treatment, diagnosis and disposition are maintained in Accordance With current Records Control Schedule 10-1 and disposal procedures are set forth in 44 U.S.C. Chapter 33. protocols.

The following are retained in CPRS/VistA: veterans full name, Social Security Number, date and place of birth, personal mailing address, personal telephone number, medical record number, race/ethnicity, system log files, sample clinical data, veteran's service connection, specific medical information related to the call.

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.*

Patient care (PHI and PII are maintained by the VistA system until archived or patient expiration. These are normally backed up and saved into an archival database according to Records Control Schedule 10-1 and VHA HANDBOOK 1907.01 for a period of 75 years. *https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf*

The TRM Plus records are to be maintained indefinitely as long as necessary in the Veterans Health Information Systems and Technology Architecture (VistA) System. Whenever technically feasible, all records are retained indefinitely in the event of additional follow-up actions on behalf of the individual. VA Electronic Health Records (EHR) system permanently retains data as part of ongoing healthcare.

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?

Official record held in the office of record. Temporary; destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. (GRS 1.1, Item 010 *https://www.archives.gov/))* (DAA-GRS-2013-0003-0001) https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

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

For TRM Plus, there is no paper record documented for a veteran. The Electronic health **Record follows prescribed criteria after a patient is no longer active. The TRM Plus records are to be maintained indefinitely as long as necessary; the records are all electronic (no paper). No records have ever needed to be destroyed, whenever technically feasible, all records are retained indefinitely in the event of additional**

follow-up actions on behalf of the individual. VA Electronic Health Records (EHR) system permanently retains data as part of ongoing healthcare.

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.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

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

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

Live patient data is prohibited during training. There is a specific "Test VistA" that will be used for training and research of product purposes. In cases of research for Telehealth a direct review of the Telehealth process and procedures would need to be accomplished.

TRM Plus Patches (VistA KIDS build and GUI executable) are released Nationally for installation prior to testing. With an approved MOU (Memorandum of Understanding) from the IOC (Interoperability Operational Coordination) site(s), the vendor, Document Storage System (DSS Inc.), Test Patches are installed and tested in the VistA and TRM Plus Pre-Production Test System. IOC site(s) tester(s) complete the Test Site(s) User's Acceptance VistA Pre-Production System document prior to VistA and TRM Plus Production System installation.

New TRM Plus Patches are released for National installation after the IOC Test Site(s) User's Acceptance VistA Production System document(s) are received.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: No data to store within the TRM Plus System. The data is stored within CPRS/VistA. The normal risk is associated with the information could be compromised or breached in the Veterans Health Information Systems and Technology Architecture (VistA) System. The only risk identified with storage, maintenance and disposition would be catastrophe failure. In the event of total continental geographic disaster. All storage electronic VistA systems have at least four storage redundancy locations. These cover Pacific time zone, Mountain time zone, Central Time zone and East time zones. So, in the event one area/time zone went down the others would pick-up the storage or retention.

Mitigation: All Veterans Health Information Systems and Technology Architecture (VistA) Systems are stored on an milli-second basis to a shadow system. This shadow is then saved to a set of off-site systems. These systems are in the various time zone of the continental United States. Each is interconnected as to have a up to the minute retrieval or re-recreation and setback to the original state of functioning.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans' Health Administration	Triage symptoms as reported by patient. Patient information is documented in a VistA progress note.	System log files, sample clinical data that may contain Protected Health Information (PHI), Person Full Name, SSN, DOB, Personal Mailing Address, Telephone Number, Medical Record Number, Emergency Contact Information, Current Medications, Race/Ethnicity, Veteran's Service Connection, Specific medical information related to the call/visit	Electronically pulled from VistA through Computerized Patient Record System (CPRS)

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. (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:

Privacy Risk: The privacy risk associated with maintaining PII/PHI is that sharing data within the Department of Veteran's 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.

Mitigation: The principle of need-to-know is strictly adhered to by the population Healthcare and non-Healthcare providers. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system. Users are trained how to handle sensitive information by taking VA Privacy and security awareness training and reading and attesting they understand the VA Rules of Behavior on an annual 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***
N/A - No external sharing				

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: There is no external sharing.

Mitigation: There is no external sharing.

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.

Each triage call begins with the notification that will be encountering a live medical person. This process begins with them verifying their authenticated items. Then a discussion of the privacy policy is instituted at first contact. All data in TRM Plus is secondary data, displayed from the VistA data contained in the Electronic Health Record. The VistA data is generated as part of routine medical care. Veterans are provided with Privacy Act statements as part of routine medical care. Additional notice is provided by the system's System of Record Notice (SORN), Veterans health information systems and technology architecture (VistA) Records VA SORN 79VA10. A third form of notice is provided by this Privacy Impact Assessment, which is available online as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii). https://www.oprm.va.gov/docs/Current_SORN_List_12_23_2020.pdf

The VistA data is generated as part of routine medical care. Veterans are provided with Privacy Act statements as part of routine medical care. All enrolled Veterans and Veterans who are treated at VA Medical Centers but not required to enroll are provided the VHA Notice of Privacy Practices (NoPP) every three years, or sooner if a change necessitates an updated notice. The NoPP is also prominently posted in every VAMC (posters) and on the VA public-facing website. Link to VHA NoPP: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

Notice is also provided in the Federal Register with the publication of the following SORNs associated with this system:

SORN 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA) Records–VA" https://www.govinfo.gov/content/pkg/FR-2020-12- 23/pdf/2020-28340.pdf.
SORN 24VA10A7 "Patient Medical Record-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

SORN 121VA10 "National Patient Databases-VA"
https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

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

Notice was provided as indicated in question 6.1a above

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.

Please see the response to 6.1a above for details

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.

Yes. A veteran is not denied service but rather is asked to comply as to provide the best service that can be given. If they do not comply treatment of presented issues will not be fully provided. Rather, the veteran will be informed they cannot be treated for any symptoms or issues which a provider is not aware of. In addition, treatment for a problem or verifying an issue cannot be accomplished.

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.

Yes. The veteran is advised of the purpose of collection information is for proper disposition. Any disclosure of this information is documented in the Electronic Health record and will not be disclosed otherwise. The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

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:

Privacy Risk: **If notice isn't provided then individuals will unknowingly be giving up their information that will be used for other purposes.**

Mitigation: **To prevent any inaccurate data, only authorized VA clinical personnel have access to the information. Notice is provided by SORN 79VA10 and all individuals should check their local VA facilities VistA PIA for more information regarding notice and consent (if applicable).**

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.***

VHA Directive 1605.01 Privacy and Release Information', section 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

7.1b 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 Privacy Act provisions.

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 information in the system falls under Privacy Act systems of record and individuals have a right of access to request a copy of the information about themselves.

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.

Under the jurisdiction of VHA, VHA Directive 1605.01 Privacy and Release Information', section 8 states the rights of the Veterans to amend their records. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. 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 Privacy Office/FOIA 1-877-750-3642 /1-877-750-3642, email: privacyservice@va.gov.

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.

Notification for correcting the information must be accomplished by informing the individual to whom the record pertains. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations who had previously received the record about the amendment. If 38 U.S.C. 7332- protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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.

> **Notification for correcting the information must be accomplished by informing the individual to whom the record pertains. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations who had previously received the record about the amendment. If 38 U.S.C. 7332- protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request**.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: **There is a risk that the individual accidentally provides incorrect information in their correspondence.**

Mitigation: **Veterans provide information at the local VAMC. Any validation performed would merely be the Veteran 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 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?

Users are granted access to TRM Plus via two methods. First, they must be added via VistA Secondary and Primary Menu's. These are given after proper request is submitted via VistA access methods. I.e., ePAS, ECAR or local access requests. The second area is via Windows Active Directory security groups. This group is only given by OI&T after a proper submission is made by the supervisory TRM Plus Manager using: I.e., ePAS, ECAR or local access requests. For new application user's Veterans Health Information Systems and Technology Architecture (VistA) System account and the new application user have completed the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training.

OI&T Technical staff:

- **ePAS approval for System Administrator, Application Administrator, VistA Management permission.**
- **Talent Management System (TMS) Inform Security for IT Specialist, Information Security for System Admin, Elevated Privileges for System Access, and VA Privacy and Information Security Awareness and Rules of Behavior Training.**
- **Non-Mail enabled account (NMEA) and associated token (USB/OTP) to access the servers.**

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 TRM+ servers/applications.

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.

TRM+ requires application-specific VistA Menu options and security keys to retrieve, create and store data in VistA.

Regular Users: Can triage the patient, pull up patient information, create notes, schedule appointments, dispositioning.

Admin Users: Can perform the same tasks as a regular user but they can also run/create reports, modify the TRM application environment via the application INI file in which they have an admin tab within the application to do so.

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.

No. Contractors and vendors do not have access to TRM+ servers/applications.

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 that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB (for AITC technicians) 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 TMS. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual HIPAA, Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

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

8.4a If yes, provide:

1. *The Security Plan Status:* Jan 25, 2022
2. *The System Security Plan Status Date:* Complete
3. *The Authorization Status:* Authority to Operate (ATO)
4. *The Authorization Date:* May 21, 2020
5. *The Authorization Termination Date:* April 14, 2025
6. *The Risk Review Completion Date:* Sept 5, 2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

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 (MBAs), 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)*

System does not use cloud technology.

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.*

System does not use cloud technology.

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.

System does not use cloud technology.

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.

System does not use cloud technology.

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).

System does not use RPA technology.

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

ID	Privacy Controls
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 they provided in this Privacy Impact Assessment is true and accurate.

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2024.07.11 13:54:25 -04'00'

Privacy Officer, Dennis Lahl

ROLAND PARTEN Digitally signed by ROLAND PARTEN
Date: 2024.07.11 14:33:50 -05'00'

Information System Security Officer, Roland Parten

TONY SINES Digitally signed by TONY SINES
Date: 2024.07.12 10:12:52 -05'00'

Information System Owner, Tony Sines

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).

VHA Handbook 1605.04, VHA Notice of Privacy Practices:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

SORNs:
Veterans' Health Information Systems and Technology Architecture (VistA) Records - VA 79VA10 https://www.govinfo.gov/content/pkg/FR-2020-12- 23/pdf/2020-28340.pdf

Patient Medical Record – VA
24VA10A7 https://www.govinfo.gov/content/pkg/FR-2020-10- 02/pdf/2020-21426.pdf

National Patient Databases – VA
121VA10 https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

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