Privacy Impact Assessment for the VA IT System called:

Women's Information & Services Engine (WISE)

Veterans Health Administration (VHA)

Veterans Relationship Management (VRM)

eMASS ID #WISE 2486

Date PIA submitted for review:

05/08/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Albert Estacio	Albert.Estacio@va.gov	909-583-6309
Information System Owner(s)	Grace Thay	Grace Thay@va.gov	202-894-0922

Abstract

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

Customer Relationship Management Women's Information & Services Engine – Optimization (CRM WISE) provides on-demand access to information about a variety of VA services and benefits and outreach to women Veterans about their VA Health benefits.

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?
Customer Relationship Management Women's Information and Services Engine (CRM WISE) is owned by Veteran Relationship Management (VRM)

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
VHA's Women Veterans Call Center (WVCC) requests a replacement application allowing its contact representatives to better support women Veterans seeking VA benefits and services information. The representatives respond to inquiries and perform outreach through inbound and outbound calls. This implementation includes the Dynamics 365 Customer Service Workspace application with Omnichannel (chat, text messaging, and telephony) features. This technical stack will allow:

- multiple ways for the Veteran to contact the WVCC, and
- provide a modernized application representatives will use to work each case/call.

We will use the Chat channel which is a widget that sits on Power Pages. Power Pages are enterprise websites built on the Microsoft Power platform.

C. Who is the owner or control of the IT system or project?
This system is owned and operated by VA's Office of Information Technology (OIT)

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?

The WVCC is an anonymous contact center and does not require end-users to provide any information in exchange for assistance/support. There are a few typical client types: women Veterans seeking a VA Healthcare referral; women Veterans seeking support connecting to another VA LOB (benefits, enrollment, Crisis hotline, etc.), women Veterans requesting general information to be sent, and women Veterans who are outreach campaign targets.

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

CRM WISE collects limited PII/PHI to assist in initiating health care referrals to the Women Veteran Program Manager (WVPM). Collection of this information is necessitated by voluntary permission of the Veteran. The WVCC is an anonymous call center and does not identity proof at this time.

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

Provides a modern, customer experience focused desktop application for our WVCC call center agents to provide information and conduct outreach campaigns accurately and quickly for our Veterans. It also allows for note taking and Veteran interaction history, allowing VA agents to provide accurate and timely responses to Veteran women. The system will ingest VA Profile, MPI, Member Services and Enrollment/Utilization data sets through SSIS package data retrieval from the VA's CXI data lake. In the future, it will interface with CTI (CISCO) and SMS functionalities.

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?

Call center agents will use CRM WISE at the VISN 5 (Canandaigua, NY) WVCC location.

3. Legal Authority and SORN

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501.
113VA10 / 88 FR 322 - Telephone Service for Clinical Care Records-VA

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 system of record notices do not require amendment.

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:

None of these data elements are required

- ☒ Name
- ☒ Social Security Number (last 4 only)
- ☒ 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 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 data elements:

- Record identification
- VA Profile ID
- Call Notes
- VHA User Name (Windows ID)

PII Mapping of Components (Servers/Database)

WISE consists of2 key components

Server: **Because we use MS platform on cloud we do not have on premise servers**

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

Database:

WISEDB

Hosted in a cloud environment of the Azure cloud

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**
MS Dynamics 365 lower environments: Dev, Dev2, INT, Test/QA, and UAT/Training. ***No PII/PHI in these environments.***	No	No	None	PII not collected in the lower environments	N/A, these environments contain test data.
MS Dynamics 365 upper environments: Pre-Production, Hot-Fix, and PROD	Yes	Yes	DOB Last4SSN Name Phone Personal Email	WVPM referrals (healthcare referrals that assist the WVPM locate the Veteran to further assist)	PII will be safeguarded according to VA best practices and handling guidelines

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?

The information comes from the Veteran or from systems already storing Veteran information: VA Profile Business Team (generates an Ad Hoc report with VA Profile and MPI data); Member Services (generates Veteran healthcare enrollment status data), and CXI (provides access to VA Profile and MPI data).

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.
The information received from sources other than the Veteran all come from internal VA data sources (see 1.2a and 1.2c) and are used for outreach and healthcare referrals

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

The information comes from the Veteran or from systems already storing Veteran information: VA Profile Business Team (generates an Ad Hoc report with VA Profile and MPI data); Member Services (generates Veteran healthcare enrollment status data), and CXI (provides access to VA Profile and MPI data).

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 Women Veterans Call Center (WVCC) will use CRM WISE dually. In some instances, data will be collected from reports generated from other internal VA systems and in other cases data is being collected by VA employees using the CRM WISE interface as they interact with callers.

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 will not be collected on a from; an OMB number is not applicable.

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.

The information is provided by the subject themselves and therefore it is assumed to be accurate.

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, Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, November 2000

SYSTEM NAME AND NUMBER: 113VA10 / 88 FR 32289 Telephone Service for Clinical Care Records-VA

PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Where application collect 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: Application mitigates the risk of identity theft by requiring all applicable Contractors and VA employees who engage with CRM WISE to complete all of the following data security and privacy 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.

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>>	File Identification purposes	Not used
Women Veterans or Dependents	• Record identification VA Profile ID (unique identifier) • First Name • Last Name • Middle Name • Maiden Name • Date of Birth • Phone Number (all phone numbers available) • Cellular • Home • Last 4 SSN (if available) • Address Line 1 • Address Line 2 • Email Address • City • State • Postal code • Country • Gender • Branch of Service • Time Served • VA Healthcare Enrollment Status Call Notes	Not used (Internal use only)

VA Employees	• First Name • Last Name • Middle Name • Phone Number (all phone numbers available) • Cellular • Work • Home VHA User Name (Windows ID)	Not used (Internal use only)

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 CRM-WISE are various management, tracking and follow-up report data used to assist in the management and operation of the Women Veterans Call Center (WVCC). Microsoft CRM has internal tools to generate graphs and reports of specific data.

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.

Application does not create any new information about the Veterans who initiate contact. Rather, in the case of a WVPM referral and if the Veteran agrees, limited information is provided to the VA's WVPM.

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?

Access to system is limited, requires PIV; and access to system and components are audited in accordance with VA 6500. The information received from the VA systems identified are encrypted during transmission, and all data is encrypted during communication from a call agent's desktop to all VA endpoints.

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

Contractor 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?

The mission of the project is to deliver exceptional customer service to the Veterans and the information stored in the system is used to create a record of a Veteran to ensure timely and accurate assistance is given. Access is determined by the program and upon approval, 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). Needed access / Approved submitters request access via Service Now with the needed roles.

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*

In order to meet the VA's goal to provide seamless customer support, all information above (provided the Veteran is willing to share the data since the call center is anonymous), in section 1.1, is retained as the WVCC Agents use the contact history that is maintained in the CRM WISE database to facilitate the Veteran's calls. This also will allow for WVCC call agents to pick up where another agent left off when a Veteran calls in.

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.*

As stated in the SORN: Policies and practices for retention and disposal of records:
Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, VHA Records Control Schedule 10–1, Item Numbers 1930.2 and 1930.4.

- Records Control Schedule: Record Control Schedule (RCS) VB-1.
- Section: Nothing is applicable – it uses other application data for viewing purposes only.
- Retention/Disposition: Information is retained for three years.
- Information is retained for three years, in accordance to Record Control Schedule (RCS) VB
- Additional RCS VB-1 links: Policy Doc 1, Policy Doc 2

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?

Records Control Schedule (RCS) 10-1 The link to the RCS is as follows:

https://www.va.gov/vhapublications/rcs10/rcs10.1.pdf
OI&T RCS 005-1.

RCS VBA-1

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

Yes, follows *RCS VB-1*

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.

It is VA policy that all Federal records contained on paper, electronic, or other medium be properly managed from their creation through their final disposition, in accordance with Federal laws, the General Records Schedule (GRS) and the VHA Records Control Schedule (RCS) 10-1. The GRS can be found on the National Archives and Record Administration website. The VHA RCS 10-1 is the

main authority for the retention and disposition requirements of VHA records. The RCS 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 record, in addition to program and service sections. No additional procedures for elimination of SPI have been established at this time.

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.

Only approved for testing mock data (false Veterans) are used when testing by those not cleared to access or view live Veteran data. This limits PII to only those who need to see it and can do so, based on their job duties. No data is used for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (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 CRM WISE may be retained for longer than necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached. No live data is used for research, testing, or training.

Mitigation: To mitigate the risks of information retention, CRM UD-O adheres to NARA Records Control Schedule. When a records retention date is reached, the individuals' information is disposed of by the method described in RCS 10.

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***
MS Dynamics 365 currently on Dev, no PII/PHI in this environment.	N/A, this environment contains test data only.	N/A	N/A

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (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: Privacy information may be inadvertently released to unauthorized individuals.

Mitigation: CRM-WISE adheres res to information security requirements instituted by the VA OIT. Contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.

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

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	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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: N/A

Mitigation: N/A

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 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.

Information is collected directly from the Veteran, is completely voluntary, and agent is required to provide a verbal notice to callers before the contact begins.

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

Information is collected directly from the Veteran, is completely voluntary, and the call center and the agent is required to provide a notice to callers before the contact begins.

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 VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

Notice is also provided in the Federal Register with the publication of the SORN:

(https://www.oprm.va.gov/privacy/systems_of_records.aspx).
113VA10 / 88 F R 32289 Telephone Service for Clinical Care Records-VA

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.

VHA Handbook 16 05 .1 Appendix D 'Privacy and Release Information', Section 5 lists the rights of Beneficiaries to request the VHA to restrict the use and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. The caller is not required to provide specific information before action can be taken, such as SSN. Callers have the right to refuse to disclose their SSNs to the VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA a 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.

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.
Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

6 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:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records, The NOPP is also available at all VHA medical centers from the facility Privacy Officer.
The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

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.***

As specified in the SORN, 2023-10732.pdf (govinfo.gov)Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system

manager in writing as or may write or visit the VA facility location where they normally receive their care.
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)?

System is a privacy act system of records

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?

N/A it is in a privacy act system of records

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.

Veteran callers are not required to provide any of their information. If they chose to correct information, they may contact the WVCC or provide the update during the service call.

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.

As stated in the SORN 2023-10732.pdf (govinfo.gov)Individuals seeking to contest or amend records in this system pertaining to them should contact the system manager in writing as indicated above. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

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.

Veteran callers are not required to provide any of their information. If they chose to correct information, they may contact the WVCC or provide the update during the service call.

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 members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: the risk of incorrect information in an individual's records is mitigated by authenticating information when possible, Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
The NOPP discusses the process for requesting an amendment to one's records.

The*]* Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.
In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

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?

Approved system personas and roles with a "need to know" who have complied with VA privacy polices and guidelines/trainings will be granted access to the system. Access is made available with an approved VA SNOW ticket, provisioned access. Once access is initiated, monitoring will ensure proper access to the system:

- Verification of the users have appropriate access levels based on the roles and responsibilities (read, write and delete)
- Routine review the WISE Usage Logs to identify any unauthorized or unusual activity, helping to detect any potential security lapses
- Routine audits of system accounts
- Deactivation of any inactive accounts to reduce adverse security impact
- Remain abreast of new and evolving VA privacy policies and regulations to ensure user management practices are in compliance

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?

Users from external agencies will not have access to the WISE system. WISE is operated and maintained in the VA OIT framework.

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.
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 their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. 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

8.2 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, the developers and other project team members are contractors. However, they are generally developing using test environments and not using live Veteran data to test and develop. All contractors are required to pass the standard VA procedures for onboarding. The appropriate contracting measures have been enacted through the VA's Contracting Office for both hosting and development contracts. Yes, this has been validated and confirmed.

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 their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and
Security training. 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?

8.4a If Yes, provide:
1. The Security Plan Status: <<ADD ANSWER HERE>>
2. The System Security Plan Status Date: <<ADD ANSWER HERE>>
3. The Authorization Status: <<ADD ANSWER HERE>>
4. The Authorization Date: <<ADD ANSWER HERE>>
5. The Authorization Termination Date: <<ADD ANSWER HERE>>
6. The Risk Review Completion Date: <<ADD ANSWER HERE>>
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH): <<ADD ANSWER HERE>>

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.
08/09/2024

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)*

All Dynamics 365 CRM applications are hosted in Microsoft Azure Government (MAG).

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.*
Service Provider: Microsoft Azure, Contract No. 47QTCA22C003G

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.

No ancillary data is collected by this application.

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.

Microsoft is responsible for Azure and maintains, validates, and monitors all security efforts inside of Azure.

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).

Does not use Robotics Process Automation (RPA)

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.05.23 13:06:48 -04'00'

Privacy Officer, Nancy Katz-Johnson

ALBERTINO ESTACIO

Digitally signed by ALBERTINO ESTACIO
Date: 2024.05.30 08:28:38 -07'00'

Information System Security Officer, Albert Estacio

GRACE THAY

Digitally signed by GRACE THAY
Date: 2024.05.23 12:40:43 -04'00'

Information System Owner, Grace Thay

APPENDIX A-6.1

Veterans contacting the WVCC receive the following notices:

Type of Contact	Type of Notice	Message
Calls	Verbal	"This call may be monitored or recorded for quality purposes."
Chat	Written	"As a reminder, this chat is anonymous. Please do not include Personally Identifiable Information (PII) in our chat, such as social security number or date of birth. This conversation may be monitored or recorded for quality purposes."
Text	Written	"This text is anonymous. Please do not include Personally Identifiable Information (PII), such as social security number or date of birth. This conversation may be monitored or recorded for quality purposes."

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 Directive 1605.04: Notice of Privacy Practices