SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements
under the Federal Information Security Management Act (FISMA).

VA HANDBOOK 6508.1: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," July 2015, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=810&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

Member Services (MS)

Veterans Benefits Administration

Veteran Centered Experience (VCE) Enterprise Access

Products (EAP)

Date PIA submitted for review:

04/06/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	tonya.facemire@va.gov	(202) 632-8423
Information System Security Officer (ISSO)	Thomas Orler	Thomas.Orler@va.gov	709-938-1247
Information System Owner	Stefano Masi	Stefano.Masi@va.gov	860-681-9927

Abstract

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

The Department of Veterans Affairs (VA) Member Services (MS) program has a goal to deliver community care through a single consolidated program that is easy to understand, simple to administer, and meets the needs of Veterans, their families, community providers and VA staff. MS represents a group of resources within various national contact centers that respond to health benefits, eligibility questions, and billing inquiries from Veterans and their families. MS is organizationally aligned under the Department of Health Operations (DHO), Veterans Health Administration (VHA). Its primary line of business is contact management support for Veterans, family members, members of the public, and payroll administration services for selected organizations within VA.
The scope of this effort is to build and deploy a new MS CRM system based on the Microsoft Dynamics 365 platform that will provide the MS service centers the ability to better support and resolve inbound calls and achieve first call resolution. This capability will include, but not be limited to: efficient workflows, streamlined business processes, incorporation of common enterprise services, adopting capabilities from the enterprise CRM platform, improved management reporting, and enhanced administrative capability that's easier to administer.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*

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

The mission of the Department of Veterans Affairs (VA), Office of Information and Technology (OI&T), Enterprise Program Management Office (EPMO) is to provide benefits and services to Veterans of the United States. In meeting these goals, OI&T strives to provide high quality, effective, and efficient Information Technology (IT) services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' healthcare in an effective, timely and compassionate manner. VA depends on Information Management/Information Technology (IM/IT) systems to meet mission goals.

The Enterprise Veterans Operations (EVO), was established in 2010 in order to provide on-demand access to comprehensive VA services and benefits in a consistent, user-centric manner through a multi-channel Virtual Call Center (VCC) processing framework. This framework is aimed to enable clients to find uniform information about VA's benefits and services regardless of the access channel used to complete their transactions with VA and to quickly identify Veterans without having to repeat information while allowing seamless access to multiple VA service lines.

Agent-assisted interactions have been the focal point of the EVO CRM effort because it is currently the most commonly used channel. The key to achieving the quality of service expected by VA clients when communicating with contact center agents is to modernize contact center capabilities and provide agents with a view of Veteran's data to triage the most common inquiries from a single Graphical User Interface (GUI) to increase first contact resolution. Similarly, important to VA's ability to measure and improve service delivery is the ability to capture information about Veterans' (and Veteran beneficiaries and representatives) interactions with VA across the VA Enterprise.

The MS Customer Relationship Management (CRM) system is owned by MS within the VHA Department of Health Operations and provides solutions for the lines of businesses (LOB) managed under the MS program that includes:

Health Benefits (HB)
The national call center for Veteran Health Benefits. Health Benefit general inquiries currently account for approximately 1/6 of the HRC's call volume.

Health Resource Center (HRC) Outbound
HRC's outbound call campaigns provide services and information to Veterans. One example is Welcome to VA (W2VA), which is a new HRC initiative and a sub line of business to the Health Benefits line of business. W2VA objective is to call and assist newly enrolled Veterans to schedule their initial appointment at a VA facility.

First Party (FP)
Handles billing inquiries and processes credit card payments.

Clinical Pharmacy Services (CPS)
Provides tier 2 support to the Consolidated Patient Account Centers (CPAC) and FP tier 1 agents for inquiries about pharmaceutical-related billing inquiries.

Pharmacy Customer Care (PCC)
Handles pharmaceutical inquiries.

Consolidated Patient Account Centers (CPAC)
Provides support for billing inquiries and make determinations on whether or not Veterans are being billed correctly.

Help Desk Support (HD)
Handles inquiries and provides support for customer facing applications (i.e., My Healthy Vet and eBenefits)

National Call Center for Homeless Veterans (NCCHV)
Handles interactions with homeless Veterans and works with Facilities to find places for Veterans to stay.

Enrollment and Eligibility Division (EED)
Manages the intake, processing, and non-income verification of new enrollments to ensure accurate processing.

Income Verification Division (IVD)
This division compares VA received income data with income data received by the Internal Revenue Service (IRS) and the Social Security Administration (SSA) to ensure that those enrolled in category 5 and up meet the income thresholds.

Informatics Division (ID)
This division is charged with analyzing and providing insights into enrollment operations.

Quality & Training Division (QTD)
This division performs Quality Assurance EED and the IVD cases.

The goal of the system to provide Call Center and Case Management solutions to provide first-call resolution for Veterans and Beneficiaries seeking healthcare, pharmacy, and account management services. The CRM system will establish timely access to information/data, tiered communication, and escalation path for the VA customer service representative. The number of affected individuals is estimated to be approximately 135,000 veterans.

This is a national system. The Member Services CRM application has been deployed in Production to several user groups within the VHA Member Services organization, located in Topeka, KS, Atlanta, GA, Fort Riley, KS and Waco, TX.

This is a Microsoft Dynamics 365-based CRM solution, providing an efficient desktop, workflow, contact history and knowledge management capabilities. This product provides a single desktop view that will enable a 360-degree view of Veteran specific data in the areas of health benefits. Security levels are enforced throughout the applications.

This particular CRM solution will store some Personally Identifiable Information (PII) level of data as it pertains to Veteran information, especially the information needed to effectively pass Master

Veteran Index (MVI) search criteria to the MVI search services. Additional PII is also stored to properly match up veterans with data that is retrieved via the multiple integrated web services. The retrieved data from these web services is not stored in the CRM system but is displayed to the user via the CRM user interface. This data will cover health information, financials, PII and even Protected Health Information (PHI). The Member Services CRM solution will share information through a couple of web service platforms. The first, VA Enterprise Integration System (VEIS), which primarily provides Member Services with the MVI search service used to identify veterans. The second, Innovation HUB (iHUB), contains various integrations to Corporation Database (Corp DB), Health Data Repository (HDR) and the Health Eligibility Center (HEC)'s Enrollment System. The type of data shared through iHUB ranges from medical data and prescriptions to billing. The Veterans Access, Choice, and Accountability Act of 2014 (VACAA) (Public Law 113-146) Section 101 requires VA to improve Veterans' access to healthcare by allowing eligible Veterans to use eligible healthcare providers outside the VA system.

VA has legal authority to share information that falls under 38 USC 8111 and 10 USC 1104 for Military Treatment Facilities; Indian Health Services 25 USC Sections 1645, 1647; 38 USC Sections 523(a), 6301-6307, 8153; and Academic sharing agreements 38 USC 8153. The legal authorities covering CRM use of PHI and PII for medical care are Public Law 115-26, Public Law 104-191, and 45 Code of Federal Regulations (CFR) 164.506.

The CRM system implements process changes to meet the requirements of Veterans Access, Choice, and Accountability Act VACAA (Public Law 113-146) Section 101, which requires VA to improve Veterans' access to health care by allowing eligible Veterans to use eligible healthcare providers outside the VA system. To comply with this this act, solutions such as CRM are needed to improve and expand the availability of services provided to Veterans. Centers for Medicare and Medicaid (CMS) system leverages data from other systems. No changes to those systems or technologies are anticipated. CRM is not a system of record, so there is no SORN required for CRM. The system of record for the data used by CRM are other systems such as MVI, VBA, and Enrollment system, which have an existing SORN. The SORN for those systems will not require amendment or revision and approval.

The application uses Microsoft Dynamics 365 CRM functionality, UI hosting and web service cloud technology.

VA is the owner of the data. Data rights are an explicit part of the contractual agreements (including the Business Associate Agreement) between VA and the contractor operating CRM.
Security for data stored within or processed by CRM is a responsibility shared among VA and the CRM contractor, as described at a high level. The contractor's responsibility for safeguarding the security and privacy of VA data is explicit in the contract executed between the contractor and the government. The contractor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability that can compromise the security of the systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, but in no event longer than one calendar day. When the security fixes involve installing third-party patches (such as patches to the Microsoft operating system or Adobe Acrobat), the contractor will, within 10 working days, provide written notice to VA that the patch has been validated as not affecting the systems. When the contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within

one calendar day. The data stored within and processed by CRM includes PHI and PII, which are information types to which VA has assigned a high-security categorization under Federal Information Processing Standard (FIPS) Publication 199 guidelines, indicating the potential for high impact if such data is disclosed to unauthorized parties.

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Current Medications
- ☐ Previous Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integration Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Other Unique Identifying Information (list below)

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>

PII Mapping of Components

CRM MS consists of 6 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CRM MS and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Development	No	No	N/A, this environment contains test data only.		
Integration	No	No	N/A, this environment contains test data only.		
QA	No	No	N/A, this environment contains test data only.		
Pre-Prod	No	No	N/A, this environment contains test data only.		
Training	No	No	N/A, this environment contains test data only.		
Prod	Yes	Yes	1. SSN 2. EDIPI 3. ICN 4. DOB 5. Address	Veteran Identification Change of information Communication	1. Data encryption **2.** Use of IAM for user authentication and authorization

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

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

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The source of PII from a CRM perspective is the Web Services layer, which is interfaced with MVI, ESR, HDR, VBA, etc. Certain Authorized users can enter PHI/PII into the system (e.g. correct contact phone number).

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Member Services Customer Services Representatives (CSRs) or Enrollment and Eligibility Division (EED) staff members collect information from Veterans, Sponsors and Beneficiaries over the phone. This information is further validated using the Person Search function in CRM supported the in-Master Veteran Index (MVI) Service.

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

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that

receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Veterans must provide three of the four identifiers for the Customer Service Representative (CSR) or Enrollment and Eligibility Division EED staff to conduct an MVI search. This ensures the correct Veteran is associated to an interaction. Personal information from the Veteran populates into the Interaction form. The CSR or EED staff member can verify with the Veteran whether their information is correct. The CSR or EED staff member can directly change the Veterans contact information in CRM that directly updates the originating system.

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

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

- Title 38, United States Code, Section 501-Veterans' Benefits
- System of Records 121VA10A7- National Patient Database-VA
- System of Records 24VA10A7- Patient Medical Records-VA
- Join Commission National Patient Safety Goals- Goal 1: Improve the accuracy of patient identification
- VHA Directive 1906- Data Quality Requirements for Healthcare Identity Management and the Master Veterans Index Functions
- VHA Directive 1604 Data Entry Requirements for Administrative Data
- VHA Directive 1906 Data Quality Requirements for Health Care Identity Management and Master Person Index Functions
- VHA Directive 1907.09 Identity Authentication for Health Care Services
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, 2016

- VHA Directive 6300(1) Records Management

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Member Services CSRs or EED staff members assist the following customers: Veterans, their beneficiaries, dependents, pharmacy staff, clinicians and other customers that call, write, and enter VHA service centers or use VA's eBenefits portal. Member Services requests key identifiers which allow for a MVI search, assuring accurate verification of the Veteran needing assistance. This capability provides the Member Services CSRs the ability to better support and resolves inbound calls and achieve first call resolution.

Privacy Risk: Information needs to be of high quality to be useful and relevant. Five characteristics of high-quality information are accuracy, completeness, consistency, uniqueness, and timeliness. Aside from human errors (such as typos), privacy issues occur when the data is not accurate and reliable enough to ensure that the right information is provided to the right individual.
As such, the privacy risk for Member Services is that a veteran is not identified correctly and as such information given by a MS representative could be wrong, misleading or inaccurate (or someone else's data).

Mitigation: The following mitigation strategies, which combine training as well as system safeguards, help reduce the chance of a privacy breach:

- Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually. For further details, see Section 8: Technical Access and Security
- Searches on a person are centralized and require a strict set of data points from the MS representative. These are at a minimum, Social Security number and first\last name or first\last name and date of birth. Results of these searches typically return

a single record, but in the occasional case that more than one Veteran is returned; the system provides additional data points to allow for a correct identification.

There is a process by which erroneous or misidentified Veterans' data can be corrected within the Master Veteran Index thus ensuring correct identification based on all programs which are using the system.

Section 2. Uses of the Information

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

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

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

The items identified in Section 1.1 are listed below with explanations of how each type of information will be used to support HEC's business purpose:

Name: Veteran's identification
Social Security Number: Veteran's identification
Date of Birth: Veteran's identification
EDIPI: Veteran's identification
Mailing Address: Used to correspond with the Veteran
Zip Code: Part of the mailing address
Phone Number(s): Used to correspond with the Veteran
Email Address: Used to correspond with the Veteran
Medications: Used to help veterans request refills and to track orders.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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

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

individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

There are no data analysis tools utilized directly against the Member Services CRM system. However, data to support analysis and reporting is extracted from the system on a daily basis and imported into a localized HRC reporting database.

2.3 How is the information in the system secured?

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

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

Information collected from the Veteran should only be used as described in this PIA. The information collected from the Veteran and validated by MVI is necessary to complete the mission of Member Services to provide customer support to Veterans.
Access to PII is determined by line of business and job categories based on management approval. The procedures for handling PII are included in the Standard Operating Procedures. Responsibility for PII is included in the Privacy, Health Insurance Portability and Accountability Act (HIPAA), and information security training and signature of the Rules of Behavior. This training is mandatory on an annual basis. Each Member Service Privacy Officer is responsible for assuring the safeguards for the PII.
The access to PII is not recorded or tracked in CRM.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

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.

Add answer here:

Annually, contractors and VA employees must take Privacy, HIPAA, and information security training.

Privacy and HIPAA Training
This course is available in two formats, web-based and text. Annually, all employees who have access to PHI and/or VHA computer systems during each fiscal year must complete either of these course versions to meet the mandatory training requirement. This training provides guidance on privacy practices for the use and disclosure of protected health information (PHI) and Veteran rights regarding VHA data. It contains policy implementation content as described in VHA Directive 1605.01. There is a substitute for VA 10203: VA 10204, Print Version.

VA Privacy and Information Security Awareness and Rules of Behavior
VA Privacy and Information Security Awareness and Rules of Behavior (ROB) provides information security and privacy training important to everyone who uses VA information systems or VA sensitive information.

After completing this course, you will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements, and consequences and penalties for non-compliance; and explain how to report incidents.

You must electronically acknowledge and accept the ROB to receive credit for course completion. This course fulfills the annual awareness training required for all VA employees. Certificates of completion for the course apply to the Information Security and Privacy Awareness requirements and to the ROB. This course updated as needed.
Note:
* You should either take the online version of this course or coordinate with your supervisor and local TMS Administrator to get credit for attending an ISO-led presentation and signing the ROB. (TMS Administrators can use item VA 832914 to record this training for learners who attend an ISO-led training. The ISO should ensure paper copies of signed ROB are retained for one year.)
Also see Section 8: Technical Access and Security.

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

Any data returned by the MVI request is stored to facilitate call tracking. A Note field is available to Customer Service Representatives (CSRs) or EED staff members where PII and PHI could be entered as a CSR or EED staff members see necessary for Veteran service. The following information is retained within the system.

- Name: Veteran's identification
- Social Security Number: Veteran's identification
- Date of Birth: Veteran's identification
- EDIPI: Veteran's identification
- Mailing Address: Used to correspond with the Veteran
- Zip Code: Part of the mailing address
- Phone Number(s): Used to correspond with the Veteran
- Email Address: Used to correspond with the Veteran

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

It is currently set for 10 years.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

Please reference the approved RCS 10-1. https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

3.4 What are the procedures for the elimination of SPI?

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

It is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from record creation through final disposition, in accordance with Federal laws, the General Records Schedule and the Records Control Schedule (RCS) 10-1. It provides a brief description of the records and states the retention period and disposition requirements. It also provides the NARA disposition authorities or the GRS authorities, whichever is appropriate for the records, in addition to program and service sections.
Temporary documents are scanned onto optical disks and retained for 10 years. Upon expiration of the data retention period, records are destroyed in accordance with VA (Handbook 6500.1 Electronic Media Sanitization Policy) and NIST (SP800-88r1 Guidelines for Media Sanitization) record retention and Media Sanitization procedures. Media in the VA environment are sanitized following VA 6500.1 Guidelines. Media in the Microsoft CRM and government cloud are sanitized in accordance with NIST SP800-88r1 as audited by FedRAMP).

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

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

Data from CRM is not used for research, testing, or training. The data contained in Microsoft Dynamics 365 remains the intellectual property of the system owner (VA). VA may use the data for purposes as necessary to fulfill its mission.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that information could be store longer than necessary.

Mitigation: MS CRM follows RCS 10-1, and all records are stored for 10 years. Upon expiration, all retained data will be carefully disposed, as described in 3.4.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Master Veteran Index (MVI)	Veteran Identification	PII (Name, DOB, SSN, EDIPI)	Direct input by stakeholders into the CRM cloud-based system
Enrollment System Redesign (ESR)	Benefits eligibility and issue resolution	PII, PHI, and Individually Identifiable Information (III)	Direct input by stakeholders into the CRM cloud-based system
Health Data Repository (HDR)	Prescription Refill	PII, PHI	Direct input by stakeholders into the CRM cloud-based system
Health Eligibility Center (HEC) Enrollment System	Benefits eligibility and issue resolution	PII	Direct input by stakeholders into the CRM cloud-based system
Veterans Benefit Administration (VBA)	Veteran identification	PII, PHI, and Individually Identifiable Information (III)	Direct input by stakeholders into the CRM cloud-based system

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:
Privacy Risk: There is a risk that information may be released to unauthorized individuals.

Mitigation: MS CRM adheres to all information security requirements instituted by the VA Office of Information Technology (OIT). Information is shared in accordance with VA Handbook 6500. Users are authenticated by use of PIV, etc. Member Services currently does not share information with other program offices thus, no internal sharing privacy risks. Development has been completed on a report that displays interaction data using Fetch. Users will be running these reports, in SQL, from a CRM organization other than the Production CRM Org. DSNs must be created in an environment where the report is built, and a DSN of the same name must be created on the server that contains the organization that this will be running from, pointing to the production VHACRM database. This new DSN must use the read-only Reporting User: HIGH\svc_HRCDataProd

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	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.

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: PII or PHI maybe shared with unauthorized parties.

Mitigation: The CRM MS system has authentication and authorization processes which ensures that only authorized parties can see the data. Furthermore, there is currently no sharing of data externally.
The risks and mitigation strategies described in this section cover all the information (and information types) listed in section 1.1 of this document.

Section 6. Notice

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

Regarding medical information, VA provides a Notice of Privacy Practice which details how medical information of Veterans, other beneficiaries who receive health care benefits from VHA, and non-Veteran patients who receive benefits from the VHA Additional notice is provided by the system's System of Record Notice (SORN), Veterans Tracking Application (VTA)/Federal Case Management Tool (FCMT)-VA, VA SORN 163VA005Q3. 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).
The Notice of Privacy Practices can be located at
http://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3048

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

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

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?
This question is related to privacy control IP-1, Consent

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

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

Follow the format below:
Privacy Risk: Insufficient notice is provided to the Veteran.

Mitigation: Notice is given by the SORN in Section 6.1. Call Center monitoring will identify instances of insufficient notice. If these are found, a follow-up with the Veteran to clarify the notice will occur. Also, additional training to Call Center staff will be given on instances where the Veteran is not given sufficient notice.

Section 7. Access, Redress, and Correction

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

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

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this

section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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 VBA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

The information collected from individuals calling in to Member Services is used primarily for call tracking. Only call tracking information can be corrected. If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the information they are now providing supersedes the information previously provided.
All requests must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VHA to the addressed listed on the governing SORN.

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.

CSRs or EED staff members will notify the caller that they may change their information if the information presented is incorrect.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

VHA Handbook 1605.1, Appendix D: Privacy and Release Information, Section 8 states the rights of Veterans to amend their records by submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, which may be used as the written request requirement, includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that the information on file is incorrect, and individuals are unaware of how to access, redress, or correct their information. Member Services CSRs or EED staff members may not adhere to information security requirements instituted by the VA OIT.

Mitigation: Individuals are notified verbally as well as able to submit VA Form 10-5345a to access their information. They can also follow the steps in VA Handbook 1605.1 to amend their information. Both contractor and VA employees are required to take annual Privacy, HIPAA, and information security training. For further details, see Section 8: Technical Access and Security.

Section 8. Technical Access and Security

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

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

Describe the process by which an individual receives access to the system.

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

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

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Specific user roles are defined for users on the Member Services system. CSRs, Supervisors, and Facility POCs have various user roles which define which areas of the system they can see or edit. Currently, user roles are defined by business leadership. The following steps are required before any user can use the system:

- Individuals must take and pass training on privacy, HIPAA, information security, and government ethics.
- Individuals must have a completed security investigation.
- Once training and the security investigation are complete, a request is submitted for access. Before access is granted; this request must be approved by a supervisor, the appropriate Information Security Officer (ISO), and OIT.
- Developer Access
- Developers of the Member Services system are VA contractors. For details on VA contractor access, see Section 8.2.
- End-User and Tester Access
- All individuals requesting End-User and Tester access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior

Training, Privacy- and HIPAA-Focused Training and Information Security for IT Specialists Training) and must be authorized by VA Project Manager. To ensure that this requirement is met, the designated VA Project POC must submit a signed Access Request Form for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access to the Member Services Environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, Current date of completion annual required VA Training, last four digits of their Social Security Number, VA Employee or Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date.

- 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. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). The rules state the terms and conditions that apply to personnel who are provided access to, or use of, information, including VA sensitive information, or VA information systems, such as no expectation of privacy, and acceptance of monitoring of actions while accessing the system. 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. Member Services users agree to comply with all terms and conditions of the VA National Rules of Behavior (ROB) by signing a certificate of training at the end of the training session.
- All individuals requesting developer access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior Training, Privacy and HIPAA Focused Training and Information Security for IT Specialists Training) and must be authorized by a VA Project Manager. To ensure that this requirement is met, the designated Veterans Centered Experience (VCE) project Point of Contact (POC) must submit a signed Access Request From for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access to the Member Services environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, Current on VA Training, VA Employee or Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or 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.

All VA contractors that have access to the pre-production environments for development purposes sign Non-Disclosure Agreements (NDAs). Contractors will also have access to the live production system for maintenance activities. The following steps are required before contractors can gain access to the system:

- Contractors must take and pass training on privacy, HIPAA, information security, and government ethics.
- Contractors must have a completed background investigation.
- Once training and the background investigation are complete, a request is submitted for access. Before access is granted, this request must be approved by the supervisor, Information Security Officer (ISO), and OIT.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the Member Services 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.

Member Services 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?

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

The Member Services system is covered under the Dynamics 365 for Government Assessing High ATO. The VA granted this ATO on February 26, 2022. The ATO will expire on February 28, 2023. The Dynamics 365 for Government Assessing High ATO was granted by the Authorizing Official Deputy Assistant Secretary, Daniel McCune (Daniel.McCune@va.gov).

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

Member Services is hosted on the Microsoft Azure Government Cloud (MAG).

Microsoft Dynamics 365 for Government platform FedRAMP ID # F1310142515 is the same for the VA ATO ID #.

Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

VA is the owner of the data. Data rights are an explicit part of the contractual agreements (including the Business Associate Agreement) between VA and the contractor operating CRM.

Security for data stored within or processed by CRM is a responsibility shared among VA and the CRM contractor, as described at a high level. The contractor's responsibility for safeguarding the security and privacy of VA data is explicit in the contract executed between the contractor and the government. The contractor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability that can compromise the security of the systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, but in no event longer than one calendar day.

When the security fixes involve installing third-party patches (such as patches to the Microsoft operating system or Adobe Acrobat), the contractor will, within 10 working days, provide written notice to VA that the patch has been validated as not affecting the systems. When the contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within one calendar day. The data stored within and processed by CRM includes PHI and PII, which are information types to which VA has assigned a high-security categorization under Federal Information Processing Standard (FIPS) Publication 199 guidelines, indicating the potential for high impact if such data is disclosed to unauthorized parties.

The Azure for Government HIGH Information as a Service (IaaS) cloud service platform is covered under the Federal Risk and Authorization Management Program (FedRAMP) P-ATO and the VA associated Cloud Service Provider (CSP) ATO documentation.

The Azure Government General Support Global Operations Services are covered under the Microsoft – Azure for Government JAB FedRAMP ATO package ID F1209051525 and the VA associated ATO.

The Microsoft Azure Government (includes Dynamics 365) SaaS Platform services are covered under the FedRAMP ATO for Microsoft Azure.
Government (includes Dynamics 365) JAB FedRAMP ATO package ID F1603087869 and the associated VA CSP-ATO.

The VA General Support Systems are covered under the VA Regions 1-6 General Support System (GSS) ATO.

9.2 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.

N/A

9.3 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.

Yes, for all cloud deployments the VA own data and identities.

The following responsibilities are retained and accountable for security and privacy by the organization:

- Data
- Endpoints
- Account
- Access management

9.4 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2022.04.13 16:43:57 -04'00'

Privacy Officer, Tonya Facemire

Thomas J. Orler 178546

Digitally signed by Thomas J. Orler 178546
Date: 2022.04.14 08:11:46 -05'00'

Information Systems Security Officer, Thomas Orler

Stefano Masi 474380

Digitally signed by Stefano Masi 474380
Date: 2022.04.17 21:10:29 -04'00'

Information System Owner, Stefano Masi

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).