Privacy Impact Assessment for the VA IT System called:

Federal Case Management Tool (FCMT)

Veterans Affairs Central Office (VACO)

Education Veteran Readiness and Employment and Federal Case Management System

eMASS ID # 1280

Date PIA submitted for review:

06/14/24

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	tonya.facemire@va.gov OITPrivacy@va.gov	202-632-8423.
Information System Security Officer (ISSO)	Christopher Massey	christopher.massey5@va.gov	214-857-3307
Information System Owner	Freda Perry	freda.perry2@va.gov	202-8027882

Abstract

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

Federal Case Management Tool (FCMT) integrates DoD data to VA data and is a Virtual Lifetime Electronic Record (VLER) application that supports the Warrior Support (WS) Program mission to provide integrated, non-clinical case management tracking, including goal documentation, progress monitoring, client tracking, performance measurement, and staff workload monitoring for Veterans and Service Members (SM). FCMT is a web-based application that provides tracking of Service Members (SM) and Veterans as described for the Federal Recovery Coordinator Program (FRCP), severely injured / visually severely impaired (SI/VSI), Case Management for Veterans Benefits Administration (VBA), Veterans Health Administration (VHA) Liaison.

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?

Education Veteran Readiness and Employment and Federal Case Management System

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

The purpose of the program is to provide a web-based case management tracking, monitoring and documentation method for service members leaving the military, deceased as well as wounded and severely injured Veterans.

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

VA Owned and VA Operated

2. Information Collection and Sharing

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

The system contains roughly 318,248 active Service Member/Veteran (SM/V) client records with around 53,632 active contacts that are associated to those SM/V client records. Those SM/V clients are individuals that require some non-clinical case management tracking, including goal documentation, progress monitoring, client tracking, performance measurement, and staff workload monitoring.

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

This application contains data such as Service Member/Veteran (SM/V clients), contacts, Federal Recovery Coordination Program (FRCP) assists, Interagency Comprehensive Plan (ICP), Veterans Health Administration (VHA) Referrals, and VBA Casualty Cases. The system also has other supporting information for each of these items such as notes, activities, and goals.

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

.

The FCMT system communicates and shares information with a few other systems which are the Care Management Tracking and Reporting Application (CMTRA)and/or VA/Department of Defense Identity Repository (VADIR)

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?

The FCMT functionality and Microsoft Dynamics 365 Online application are hosted in Azure US Government and Dynamic 365 US Government and meet the FIPS 140-2 standard. In addition, Microsoft uses encryption technology to protect customer data in Dynamics 365 while at rest. User access is only for authorized personnel and the lowest level of security needed for the user's role is granted.

3. Legal Authority and SORN

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

Title 38 USC Section 501, Chapters 11, 13, 15,18, 30, 31, 32, 33,34, 35,36, 39, 51, 53, & 55. As required by the Privacy Act of 1974 (5 U.S.C. 552a(e)(4)), notice is hereby given that the Department of Veterans Affairs (VA) is amending a system of records in its inventory titled ''Supervised Fiduciary/Beneficiary and General Investigative Records—VA''. Records for FCMT are retained in accordance with Record Control Schedule VB-1, Part II, Central Office,, System of Record Notice SORN 163VA005Q3,), Title 38 U.S.C. 5106. United States Code. Federal Case Management Tool (FCMT) – VA - 202VA005Q / 86 FR 68721

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 is using cloud technology, the SORN for the system cover cloud usage or storage.

4. System Changes

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

Completion of this PIA will not require changes to business processes.

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

No technology changes after completion of this PIA

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☒ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below

Other PII/PHI data elements: << EDIPI- Electronic Data Interchange Personal Identifier.>>

<<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 (Servers/Database)

Federal Case Management Tool (FCMT) consists of components, are Care Management Tracking and Reporting Application (CMTRA) and Veterans Affairs Department of Defense Identity Repository (VADIR). (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Federal Case Management Tool (FCMT) and the reasons for the collection of the PII are in the table below.

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

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

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
Care Management Tracking and Reporting Application (CMTRA)	Yes	Yes	Social Security Number (SSN), Electronic Data Interchange Personal Identifier (EDIPI), Name, Address, phone, email, Date of Birth (DOB), Date of Death.	This information is collected and stored with the SM/V profile to help identify and provide the proper service and coordinated care to the SM/V.	Secure File Transfer Protocol (FTPS)
Veterans Affairs Department of Defense Identity Repository (VADIR)			Social Security Number (SSN), Electronic Data Interchange Personal Identifier (EDIPI), Name, Address, phone, email, Date of Birth (DOB), Date of Death.	This information is collected and stored with the SM/V profile to help identify and provide the proper service and coordinated care to the SM/V.	Hypertext transfer protocol secure (HTTPS)

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 primary sources of information for the FCMT Tool are Service Member/Veterans (SM/V).

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.

Service Member/Veterans (SM/V) are the primary sources of information for the FCMT Tool which is then validated against the VA/Department of Defense Identity Repository (VADIR). Upon validation, an electronic one way pull of SM/V information is initiated from those sources. The FCMT Tool also uses the National Information Exchange Model (NIEM) standards and extensions as the Canonical Data Model (CDM) for exchange of data.

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

Federal case Management does not create any new information from the collected information.

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 sources of information reviewed in FCMT are from Service Members and Veterans (SMV) through case managers initiating and/or monitoring care during treatment at VHA medical facilities. During service or after discharge, a SM/V may request care at a VHA facility.

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?

There is the Veteran or Power of Attorney (if POA form is present) completes an intake such as submitting service documents (DD 214, etc.) for eligibility of possible benefits and completing VA Form 10-10EZ. The SM/V also provides personal identifiable information to the administrative personnel, such as Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Email Address and Emergency Contact Information (Name, Phone Number, etc. of a different individual). Information may be collected in person verbally and through paper forms, as well as, through electronic documentation. There is an initial lookup VA/Department of Defense Identity Repository (VADIR) to validate the SMV and a one way pull of the information from those sources into the FCMT. FCMT information is sent and received electronically. It also uses the National Information Exchange Model (NIEM) standards and extensions as the Canonical Data Model (CDM) for exchange of data.

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

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

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

Information provided to FCMT by SM/V for the case and workload management is validated against the VA/Department of Defense Identity Repository (VADIR).

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?

The ICP system which is a functionality of FCMT provides the automated functionality to monitor the saving process and generate meaningful alerts for participants upon malfunctions or error conditions. Prior to sending the messages, the participants must review the notice and consent information and provide authorization to send the information. Information will be encrypted with digital signature.

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

To determine eligibility for VA benefits or verifying other information with respect there to GN General Number 03313.45 Used to retrieve Veteran information. Legal authority: Title 38 USC Section 501, Chapters 11, 13, 15,18, 30, 31, 32, 33,34, 35,36, 39, 51, 53, & 55. As required by the Privacy Act of 1974 (5 U.S.C. 552a(e)(4)), notice is hereby given that the Department of Veterans Affairs (VA) is amending a system of records in its inventory titled ‘‘Supervised Fiduciary/Beneficiary and General Investigative Records—VA’’. Records for FCMT are retained in accordance with Record Control Schedule VB-1, Part II, Central Office, System of Record Notice (SORN) VA (138VA005Q/74 FR 3709, System of Record Notice SORN 163VA005Q3,), Title 38 USC Section 501 Section 501(a), (b), and chapter 55 of Title 38, United States Code. Federal Case Management Tool (FCMT) – VA - 202VA005Q / 86 FR 68721

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

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

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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: Data reviewed in the FCMT Tool is classified as a mixture of Sensitive and Non-Sensitive, depending upon the source and nature of the data. There is a risk that sensitive information may be shared with an unauthorized VA program, system, or individual.

Mitigation: The VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. The overall security controls follow VA 6500 Handbook, and NIST SP800-53 rev 4 moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility' common security controls. These issues are identified and described in the system security plans for the individual information systems. Prior to sending the messages, the participants must review the notice and consent information and authorize to send the information.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system 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
First/Last Name	Used as identifier	Not used
Social security Number	Used to verify Veteran identity and as a file number for Veteran	Not used
Date of Birth	Used to verify Veteran identity	Not used
Mailing Address	Used to correspond with the Veteran	Not used
Phone Number(s)	Used to correspond with the Veteran	Not used
Email Address	Used to correspond with the Veteran	Not used
Emergency Contact Information	Used in emergencies to contact the Veteran	Not used
EDIPI	Used to verify Veteran identity	Not Used
Medical Records	Used to record the history of health and medical conditions of the veterans such as health problems, diagnosis, therapeutic	Not used

	procedures, X-rays, laboratory tests, and operations.	

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?

The FCMT system does not perform any complex analytical functionality, and it does not create an output data from such analysis. As part of the FCMT business processes, the system users will be searching for SM/V records to see if they exist when they are working on a case.

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.

The FCMT system does not perform any complex analytical functionality, and it does not create an output data from such analysis. As part of the FCMT business processes, the system users will be searching for SM/V records to see if they exist when they are working on a case. In cases where an existing SM/V record does not exist, system users will go through the process to create a new record using the Client Search and Register function within FCMT. This information is then used within the system to perform case management activities including generation of a case plan for the SM/V

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?

The FCMT functionality and Microsoft Dynamics 365 Online application are hosted in Azure US Government and Dynamic 365 US Government and meet the FIPS 140-2 standard. In addition, Microsoft uses encryption technology to protect customer data in Dynamics 365 while at rest. User access is only for authorized personnel and the lowest level of security needed for the user's role is granted.

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

PII is stored in a FIPS 140-2 compliant data structure and on an encrypted platform.
FTPS and HTTPS protocol used to protect data.

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

Data manipulation is controlled by 2-factor authentication Role-Based access to the system. Access is controlled by management.

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?

FCMT has an access procedure that is monitored by Microsoft Dynamics 365 and the FCMT Team and followed by users to make sure all controls are in place to assure the safeguard of PII information.

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

Microsoft Dynamics 365 as well as the FCMT Team are tracking user IDs as users log into the system. The FCMT Team Technical Specialist does a manual monthly review of the active users within the database. If a user has not maintained activity within 60 days, the user and business owner will be notified. At 90 days, if there is still inactivity, the user will be removed from having access to the FCMT data and will need to submit the proper request to gain access again to the FCMT application which is below.

2.4c Does access require manager approval?

Yes, manager approval is required.

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

Access to PII information is being monitored through an Audit History log per user as well as Form VA9957 which is signed by the Project Manager or System Owner.

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

Microsoft Dynamics 365 as well as the FCMT Team

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

• Name
• Social Security Number
• Date of Birth • Mailing Address
• Zip Code • Phone Number(s) • Email Address
• Emergency Contact Information (Name, Phone Number, etc. of a different individual)
• Previous Medical Records
• EDIPI

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.*** *This question is related to privacy control DM-2, If the system is using cloud technology, will it be following the NARA approved retention length and schedule? Data Retention and Disposal.*

Per Record Control Schedule VB-1, Part II, Central Office, Control files. Single and multiple entries. Cards of all types, lists and logs, used solely for convenience of control operations and reference, and prepared when local control is required by directives, or operational needs over such activities as the distribution, release and return of certain papers and forms; the progress of work form assignment to completion; follow-up on actions due within specific periods of time; and similar local control activities. INCLUDES discontinued control files. EXCLUDES control files used for fiscal and accounting purposes. VBA approved as a non-record. Per VA SORN 163VA005Q3, Veterans Tracking Application (VTA)/Federal Case Management Tool (FCMT) states, VA retains selected information for purposes of making eligibility determinations for VA benefits. The information retained may be included in the VA records that are maintained and disposed of in accordance with the appropriate record disposition authority approved by the Archivist of the United States.

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?

The information retained may be included in the VA records that are maintained and disposed of in accordance with the appropriate record disposition authority approved by the Archivist of the United States.

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

Per Record Control Schedule VB-1, Part II, Central Office, Control files. Single Destroy after control is no longer needed over the related document or action and/or no further entries can be made on the control medium. Destroy discontinued file immediately after discontinuance.
https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc

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.

To dispose of electronic records in a way that meets basic records management standards, records are eliminated (i.e., delete all copies in repositories and back-up systems) in a way that is reliable, systematic, transparent, and documented, and that avoids ad-hoc, individual decisions on what to destroy.

Records schedules may be used to authorize and carry out disposal of electronic records, provided that:

- The records schedule accurately reflects the current activities, records (including electronic), and retention requirements. Regular review of business records requirements and updating of schedules is recommended.

- The electronic records can be clearly identified with a current records schedule (and series component where applicable) and the correct disposal date can be calculated based on known end dates of the records.

- It is possible to apply the retention and disposal actions to groups (e.g., folders, document libraries) of related records governed by the same schedule. Destruction of individual documents in isolation, or in an ad hoc manner, should be avoided.

- The manager responsible for the business area has authorized this action and has assigned the task to a suitable employee. Other staff may need to assist in identifying records, but responsibility for carrying out and documenting the disposal of records should not be left to individual users/employees.

- The records are not subject to a Freedom of Information and Protection of Privacy Act- FIPPA request, litigation hold, audit, or investigation.

- The deletion is documented in a way that demonstrates due diligence and accountability for its actions. Key information captured includes:
  o Basic identification of the records destroyed
  o the applicable records schedule
  o the end date of the records

o the date the records were due for disposal under the schedule
o the date destroyed
o the signature or electronic identifier of the person who completed the deletion.

The following methods are utilized below based on an approved request submitted in ServiceNow by the Project Manager or the System Owner. The appropriate VA SORN and RCS is utilized to determine the method of disposition.

Deleting – The simplest, easiest and most appropriate method is hitting the delete key. Deleting is not the same as destroying the record; it just destroys the access to the record. The record continues to exist on the storage medium until they are overwritten – and can be recovered using digital forensics.

Overwriting – Destroying electronic records is to use software that overwrites the records. This makes the possibility that the records can be recovered much more remote than simply hitting the delete key.

Degaussing (Magnetic Media) – Exposing magnetic media (such as tapes and floppy disks) to a powerful magnetic field to scramble the data. It may take multiple passes of the magnet over the storage media to ensure that the records are properly destroyed.

Physically Destroying Storage Media – Actually physically destroying the storage media with sensitive/confidential records. Destroying records stored on portable media, such as shredding Laptops, CDs and DVDs, cutting up old floppy disks, etc.

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.

FCMT has a 'hot fix' environment (PREPROD) that contains real data. The development and support teams participate in training to ensure all team members are aware of, follow, and enforce that no PII or production data leaves the production environment.

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: The risk of retaining data with the length of time within the Federal case management Tool (FCMT) includes compromised unintentionally released, or breached data.

Mitigation: To mitigate the risk posed by information obtained, FCMT adheres to the Record Control Schedule VB-1, Part II, Central Office, System of Record Notice (SORN) VA (138VA005Q/74 FR 3709 and System of Record Notice SORN 163VA005Q3. When SMV data is reviewed, FCMT will carefully dispose of the data by the Record Control Schedule VB-1, Part II, Central Office, System of Record Notice (SORN) VA (138VA005Q/74 FR 3709 and System of Record Notice SORN 163VA005Q3.
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***
VHA Support Service Center (VSSC) Care Management Tracking and Reporting Application	VHA Support Service Center (VSSC) Care Management Tracking and Reporting Application (CMTRA) used for reporting purposes	Social Security Number (SSN), Electronic Data Interchange Personal Identifier (EDIPI), Name, Address, phone, email, Date of Birth (DOB), Date of Death.	Secure File Transfer Protocol (FTPS)
Veterans Affairs Department of Defense Identity Repository (VADIR)	Department of Defense used to monitor, track, and create SM/V client records	Social Security Number (SSN), Electronic Data Interchange Personal Identifier (EDIPI), Name, Address, phone, email, Date of Birth (DOB), Date of Death.	Electronic transferred through secured connection using Hypertext Transfer Protocol Secure (HTTPS)

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: There is a risk that information may be shared with an unauthorized VA program, system, or individual. The privacy risk associated with maintaining PII and PHI is that sharing data within the Department of Veteran's Affairs could happen and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization using Network Identification (NTID) are all measures that are utilized within the facilities. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system.

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***
None				

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***
Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

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

Follow the format below:

Privacy Risk: There is no external sharing.

Mitigation: There is no external sharing.

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.

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, which can be viewed at https://www.oprm.va.gov/docs/sorn/SORN163VA005Q3.PDF a

A second form of notice is the VA SORN 138VA005Q/74 FR 37093, Veterans Affairs/Department of Defense Identity Repository (VADIR)—VA which can be viewed at the following link 2021-26257.pdf (govinfo.gov)

Federal Case Management Tool (FCMT) – VA - 202VA005Q / 86 FR 68721
https://www.oprm.va.gov/privacy/systems_of_records.aspx

A third form of notice is provided by the Privacy Impact Assessment, which is available online as required by the eGovernment Act of 2002, Pub.L. 107–347§208(b)(1)(B)(iii).

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
A second form of notice is the VA SORN 138VA005Q/74 FR 37093, Veterans Affairs/Department of Defense Identity Repository (VADIR)—VA which can be viewed at the following link 2021-26257.pdf (govinfo.gov)

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.

Notice is provided by the system's System of Record Notice (SORN 138VA005Q/74 FR 37093, Veterans Affairs/Department of Defense Identity Repository (VADIR)—VA which can be viewed at the following link
2021-26257.pdf (govinfo.gov)

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.

VA only shares Veteran/Service Member information with specific organizations that have partnership agreements with VA and are part of VA's approved, trusted network via VHIE- Veterans Health Information Exchange. However, the Veteran or Service Member may opt out of electronic sharing by submitting VA Form 10-10164. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose information to VA. (see 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?

Per Notice of Privacy Practices IB-10-163, Veterans/Service Members have the right to review and obtain copies of health information within their records. V/SM must submit the request in writing to a facility Privacy Officer at the VHA health care facility or Central Office. V/SM may
also request a restriction, receive accounting disclosures, receive receipt of communications in a confidential manner and an amendment (correction) to information in records that is believed to be incomplete, inaccurate, untimely, or unrelated to care. The request must be submitted in writing, specify the information that needs to be corrected and provide a reason to support the request.
However, VA will not honor requests to remove all or part of the health information from the electronic database of health information that is shared between the VHA and DoD, or to restrict access to health information by DoD providers with whom the V/SM may have a treatment relationship with.

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. (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 individuals who provide information to FCMT and other sources mention in section 1.2 above will not know how their information is being shared and used internal to the Department of Veterans Affairs.

Mitigation: This PIA serves to notify individuals of the FCMT Tool and includes information about the sharing of information between FCMT and the other applications. Additional notice is provided by the system's System of Record Notice (SORN) in Section 6.1 above.

Section 7. Access, Redress, and Correction

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

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

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

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

VHA Directive 1605.01 states that requests for access to look at or review copies of individually identifiable information must be processed in accordance with all Federal laws, including 38 U.S.C 5701 and 7332, FOIA, Privacy Act, and HIPAA Privacy Rule. Except as otherwise provided by law or regulation, individuals, upon signed written request, may gain access to, or obtain copies of, their individually identifiable information or any other information pertaining to them that is contained in any system of records or designated record set maintained by VHA. Individuals do not have to state a reason or provide justification for wanting to see or to obtain a copy of their requested information.

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

Federal Case Management is not exempt from the access provision of the Privacy Act

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

Per Notice of Privacy Practices IB-10-163, Veterans/Service Members have the right to review and obtain copies of health information within their records. V/SM must submit the request in writing to a facility Privacy Officer at the VHA health care facility or Central Office. V/SM may also request a restriction, receive accounting disclosures, receive receipt of communications in a confidential manner and an amendment (correction) to information in records that is believed to be incomplete, inaccurate, untimely, or unrelated to care. The request must be submitted in writing, specify the information that needs to be corrected and provide a reason to support the request.
All information for FCMT is coming from other systems (VADIR)

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.

Veterans may request correction or amendment via submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

These processes are not performed by FCMT staff as all information for FCMT is coming from other systems (VADI).

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.

The VHA staff member who authored the information that is subject to the amendment request must review and determine whether to approve or reject the request. In reviewing requests to amend, the author must be guided by the criteria set forth in 38 CFR 1.579.

A request to amend record must be acknowledged in writing within 10 workdays of receipt. If a determination whether to honor the request has not been made within this time period, the Chief of HIM, or designee or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from the receipt of request If the anticipated completion date indicated in the acknowledgement cannot be met, the individual must be advised in writing of the

reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from the receipt of request.

All information for FCMT is coming from other systems (VADIR) with information provided by VHA and DoD.

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.

When a request to amend a record is denied, the Chief of HIM, or designee, or the facility Privacy Officer, or designee, must promptly notify the individual making the request of the decision. The written notification must:

State the reasons for the denial. VHA must deny a request to amend a record if VHA finds that the individually- identifiable information or record requested to be amended:

1. Was not created by VHA and the originator of the individually- identifiable information is another Federal agency available to act on the request. In this instance, the individual will be information that the individual needs to request that the originating Federal agency of the individually- identifiable information is no longer available to act on the request or authorizes VA to decide whether to amend the record, then VHA must do so.

2. Is accurate, relevant, complete, or timely in its current form.

3. Is not part of a VHA system of records or designated set.

Advise an individual that they can appeal to an OGC- Office of General Counsel.

Advise an individual that if an appeal is not filed and a statement of disagreement is not submitted, the individual may still request that the VHA health care facility provide the individuals request for amendment and the denial with all future disclosures of the information. The request needs to be submitted in writing to the Chief of HIM or designee, or the facility Privacy Officer, or designee.

Describe how the individual may file a complaint with VHA or the Secretary, HHS. The description must include the name or title and telephone number of the contact person or office.

Be signed by the VHA health care facility Director or official designee.

If requested by the individual, the Chief of HIM, or designee, or the facility Privacy Officer, or designee, must identify the individually identifiable information that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment and the facility's denial of the request to the individual's record.

If the amendment does not pertain to the Veteran's health record, the facility Privacy Officer will work with the appropriate System Manager for the VHA system of records in which the information is maintained following the same amendment process as above.

All information for FCMT is coming from other systems (VADIR) with information provided by VHA and DoD.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the individual unknowingly provides incorrect information upon entry.

Mitigation: Any validation performed would merely be the veteran personally reviewing the information before they send or accept it. Individuals are able to provide updated information for their records by updating the information and indicating that the new information supersedes the previous data. FCMT will rely on the originating systems process of validating and updating information. FCMT will use updated data as it's provided from the originating system.

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?

Office of Information and Technology (OIT) documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. This documentation and monitoring are performed using Talent Management System (TMS). Access to the system is granted to VA employees and contractors by the local authority within each administrative area staff office, following the described account creation process.

All individuals requesting developer access 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 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 FCMT 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.

Developers and FCMT Project teams will work to create, update, access and disable end user and tester accounts for project teams. Additionally, there shall be a review of user access periodically to evaluate whether users are active in the environment; if the user is not active, their account is terminated. A designated VA Project Point of Contact (POC) is the only person who may submit account creation requests and submitted for accountability purposes.

End Users must submit a request through form VA9957 and utilize the FCMT Access Procedure:

1. Most FCMT Access request are submitted by FCMT Business Unit (BU) Owners through tickets (Requests or Incidents) in ServiceNow and have the VA9957 form attached to the ticket. If a request comes in directly from a user, not a BU Owner, Tier II refers the user to the ServiceNow "KB0010956 - FCMT: Request a New Account/Update an Existing Account" Knowledge document and ask them to complete the VA9957 form and attach it to the ticket.
2. Once the ticket is assigned to "FCMT Product Support" ServiceNow group:
    a. One of the Tier II support person assigns the ticket to himself / herself and makes sure the VA9957 is attached and correctly filled out (the main thing is to be signed by a BU owner).
    b. Then the Tier II support person has to submit a request for D365 FCMT Provisioning / Access to Microsoft D365 Support.
    c. Microsoft D365 support request that only one ticket request be submitted per day, therefore FCMT Tier II support has to coordinate to make sure only one request is submitted.
    d. Tier II support person then fills out the "VA Dynamics 365 User Provisioning and Access V2.0 Form" listing all users who requested FCMT access during the day.
    e. Before Close of Business (COB) day (around 3PM) Tier II support person sends an email to the FCMT Access Approvers and Microsoft D365 Support with the "VA Dynamics 365 User Provisioning and Access V2.0 Form" attached.
    f. FCMT Access Approvers (System Owner and Project Manager) approve the same day by replying to all and stating that it is approved. Tier II should follow up with approvers if not approved before COB.
    g. After the request is approved, it takes 2 business days for the account to be created. Once it is created, D365 notifies requesters that the account has been created.
    h. Tier II Support person then sets up the new account by filling out the Job Title, Facility, VHA Facility (if VHA BU), Business Unit, Security Roles, Teams (if needed) and Subscriptions (if needed). Note that the Tier II support person must add

the following two security roles to all new users in addition to the roles specified in the VA9957 form: "* D365 Upgrade Process Configuration Role" and "North52 Formula Manager – Standard".

i. After the setup is completed, Tier II Support person sends an email to the New User informing that the account has been created and providing the FCMT URL and closes the ServiceNow ticket.

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 other agencies do not have access to any FCMT data.

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.

Data manipulation is controlled by 2-factor authentication Role-Based access to the system. Access is controlled by management.

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.

VA contractors supporting FCMT activities will be provided access to the FCMT development and test environments as needed. Access to the system is granted to VA contractors by the local authority within each administrative rea staff office. VA contractors will have access to the system via end-user and developer accounts.
When the VA and the contractor have entered into an agreement, the contractor must sign VA Form 0752 Confidentiality of Sensitive Information Non-Disclosure Agreement.
Contractors having access to the system will have to go through background checks/investigation done by the Office of Personnel Management (OPM) and it depends on the level needed as to the frequency of when it is done. Typically, Program Management Office (PMO) support is a Low/Tier 1 investigation and development is done at a Moderate/Tier 2 in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A. All contractors accessing the environments must comply with access and security requirements outlined in Section 8.1.

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 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). After the FCMT 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. FCMT users agree to comply with all terms and condition of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 23-Jun-2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 20-Oct-2023
5. *The Authorization Termination Date:* 19-Oct-2025
6. *The Risk Review Completion Date:* 14-Dec-2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***
<<ADD ANSWER HERE>>

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)*

Federal Case Management Tool (FCMT) is a custom code SaaS (Software as a Service) application developed to interface with the VA Microsoft Dynamics 365 (D365), hosted in the Microsoft Azure Government Cloud FedRAMP.

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

<<ADD ANSWER HERE>>

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

<<ADD ANSWER HERE>>

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

<<ADD ANSWER HERE>>

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

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

<<ADD ANSWER HERE>>

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

TONYA FACEMIRE

Digitally signed by TONYA FACEMIRE
Date: 2024.06.20 08:43:02 -04'00'

Privacy Officer, Tonya Facemire

CHRISTOPHER MASSEY

Digitally signed by CHRISTOPHER MASSEY
Date: 2024.06.20 08:24:50 -05'00'

Information Systems Security Officer, Christopher Massey

FREDA PERRY

Digitally signed by FREDA PERRY
Date: 2024.06.21 12:09:22 -04'00'

Information Systems Owner, Freda Perry

APPENDIX A-6.1

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

Notice is provided by the system's System of Record Notice (SORN), Veterans Tracking Applicatio (VTA)/Federal Case Management Tool (FCMT)-VA,VA SORN 163VA005Q3, which can be viewed at https://www.oprm.va.gov/docs/sorn/SORN163VA005Q3.PDF

A second form of notice is the VA SORN 138VA005Q/74 FR 37093, Veterans Affairs/Department of Defense Identity Repository (VADIR)—VA which can be viewed at the following link 2021-26257.pdf (govinfo.gov)

Federal Case Management Tool (FCMT) – VA - 202VA005Q / 86 FR 68721
https://www.oprm.va.gov/privacy/systems_of_records.aspx
A third form of notice is provided by the Privacy Impact Assessment, which is available online as required by the eGovernment Act of 2002, Pub.L. 107–347§208(b)(1)(B)(iii).

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
A second form of notice is the VA SORN 138VA005Q/74 FR 37093, Veterans Affairs/Department of Defense Identity Repository (VADIR)—VA which can be viewed at the following link 2021-26257.pdf (govinfo.gov)

HELPFUL LINKS:

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

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

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

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

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