Privacy Impact Assessment for the VA IT System called:

FEDERAL CASE MANAGEMENT TOOL (FCMT)

Department of Veterans Affairs

Date PIA submitted for review:

07/23/2020

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Rita Grewal</td>
<td><a href="mailto:Rita.Grewal@va.gov">Rita.Grewal@va.gov</a></td>
<td>202-632-7861</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Roland Parten</td>
<td><a href="mailto:Roland.Parten@va.gov">Roland.Parten@va.gov</a></td>
<td>205-534-6179</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Paul T. Zeien</td>
<td><a href="mailto:Paul.Zeien@va.gov">Paul.Zeien@va.gov</a></td>
<td>708-483-5432</td>
</tr>
</tbody>
</table>
Abstract

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

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, and Chapter 63 Special Outreach programs.

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.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- 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?
- Does the system use cloud technology? 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.
- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
• 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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?

The Federal Case Management Tool resides under the Veteran Benefits Administration. The purpose of the program is to provide a web-based case management tracking, monitoring and documentation method for service members leaving the military as well as wounded and severely injured Veterans. The system contains roughly 254,618 active Service Member/Veteran (SM/V) client records with around 39,477 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.

The application is a Microsoft Dynamics 365 CRM cloud-based system running within the Microsoft Government Community Cloud (GCC). This application contains data such as 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. The FCMT system communicates and shares information with a few other systems which are the Master Veteran Index (MVI) and/or VA/Department of Defense Identity Repository (VADIR) and VA Data Access Service (DAS).

When using the system for looking up a SM/V client to check on or start a new case, communication is sent and received to and from the Master Veteran Index (MVI) and/or VA/Department of Defense Identity Repository (VADIR). Upon validation, an electronic one way pull of SM/V information is initiated from those sources. In addition, the FCMT system is integrated into the Department of Defense (DoD) Case Management System (CMS) by means of the VA Data Access Service (DAS) interface. FCMT pushes data to and receives data from the DoD CMS system in relation to SM/V ICP data. There are various use cases for different scenarios that require data exchange to ensure each agency has all information needed to properly service the SM/V without any gaps in information.

Being a government cloud-based system, VAEC Azure Government Cloud, FCMT contains a consistent level of access security and controls that manage the entire community. The Microsoft Government Cloud does include a high impact FedRAMP authorization. The way PII data is protected and handled is consistent given this cloud infrastructure, with the same security controls. The completion of this PIA should not result in any changes to the business processes and should not result in technology changes.
In the event of any disclosure of PII data from the FCMT system, there would be a loss of confidence in the ability of the Department of Veterans Affairs (VA) to protect data, as well as in Microsoft as the CSP for the application. Disclosure of such data could also result in financial impact as with any breach in PII data. As such user access runs through an approval process and users are granted lowest security role access for the job functions, they fulfill. User access is also audited, and user accounts are removed when they are no longer needed. SORN VA (138VA005Q/74 FR 37093), Authority for maintaining this system is Title 38 U.S.C. Section 5106. The Department of Veterans Affairs (VA) is amending a system of records in its inventory titled “Supervised Fiduciary/Beneficiary and General Investigative Records—VA.

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.

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
- Other Unique Identifying Number (list below)
EDIPI- Electronic Data Interchange Personal Identifier

PII Mapping of Components

Federal Case Management Tool (FCMT) consists of one key component, the Microsoft Dynamics 365 Online application.

PII Mapped to Components

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Dynamics 365 Online application</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, SSN, DOB, Personal Mailing Address, Personal Phone Number, Emergency Contact Information, Previous Medical Records, EDIPI- Electronic Data Interchange Personal Identifier</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

Service Member/Veterans (SM/V) are the primary sources of information for the FCMT Tool which is then validated against the Master Veteran Index (MVI) and/or 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.

1.3 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.

The sources of information reviewed in FCMT are from Service Members and Veterans (SM/V) 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. There 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 in either the Master Veteran Index (MVI) or 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 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose. This question is related to privacy control AP-2, Purpose Specification.

The purpose of the information is to:
- Support coordination between all the different care providers
- Allow SM/V to view and track all coordination plan
- Establish interoperability with the VA so that all members of the Case Management team (CMT) regardless of the Department are able to see the same case information
- Provide the exchange of a common care plan between the DoD and the VA
- Provide a more synchronized process to deliver care to Service Members

1.5 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.

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

1.6 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.

1.7 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.

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’s 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 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.

- Name: Veteran’s identification
- Social Security Number: Used to verify Veteran identity and as a file number for Veteran
- Date of Birth: Used to verify Veteran identity
- 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
- Emergency Contact Information (Name, Phone Number, etc. of a different individual): used in emergencies to contact the Veteran
- Previous Medical Records: Used to record the history of health and medical conditions of the veterans such as health problems, diagnosis, therapeutic procedures, X-rays, laboratory tests, and operations.
- EDIPI: used to verify Veteran identity

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.

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. When the case and plan also applies to the DoD, an action can be made to share this data with the DoD using the Interagency Case Plan (ICP) Exchange.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. 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. 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.

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. Microsoft Dynamics 365 as well as the FCMT Team are tracking user IDs as users log into the system. 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. 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.

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 requests 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.
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

The information listed in Section 1.1 is retained in the Federal Case Management Tool (FCMT database.
• 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

Note: This is only being stored if the SM/V is not in Veterans Affairs/Department of Defense Identity Repository (VADIR)/ Master Veteran Index (MVI).

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, 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)? 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.

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 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

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. 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

The FCMT non-production environments do not contain any real data. All the lower environments contain test data which is created for test purposes. No real PII from production is brought down or used in the lower environments at any time. 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.

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 to retention and obtaining data within FCMT Tool is the longer information is that information can be compromised, unintentionally released or breached. FCMT does a one way pull for information but does not store in the system.

**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. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Veteran Index (MVI)</td>
<td>Master Veteran Index (MVI) for registration of clients and on-demand refresh of demographics</td>
<td>ICP Pulls all data types such as Name, date of birth (DOB), gender, address, phone number, e-mail, SSN.</td>
<td>SOAP (Simple Object Access Protocol) using Hypertext Transfer Protocol Secure (HTTPS)</td>
</tr>
<tr>
<td>Benefits Gateway Services (BGS)</td>
<td>Benefits Gateway Services (BGS) for viewing real-time benefit and payment data from various VA systems.</td>
<td>ICP pulls read-only data (such as compensation/ratings claim history and status for each claim, payment history) from the Corporate Database</td>
<td>SOAP (Simple Object Access Protocol) using Hypertext Transfer Protocol Secure (HTTPS)</td>
</tr>
</tbody>
</table>
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 data element types such as PII/PHI that are shared/received 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 | ICP pushes data to VSSC/CMTRA on nightly basis via FCMT. Data includes name, social security, DOB, mailing address, zip code, phone number and email addresses | SOAP (Simple Object Access Protocol) 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. 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: This question is #7 in the Privacy Threshold Analysis.

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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoD Case Management System (Department of Defense)</td>
<td>Department of Defense used to monitor, track and create SM/V client records</td>
<td>ICP record contains the name, social security, DOB, mailing address, zip code, phone number and email address of Veterans being</td>
<td>VADIR- FCMT IS A MOU v1.8 Additional notice is provided by the system’s System of Record Notice (SORN) VA</td>
<td>Electronically transferred through secured connection using Http (Hypertext Transfer Protocol)</td>
</tr>
<tr>
<td>Identity Repository VADIR</td>
<td>Department of Defense used to monitor, track and create SM/V client records</td>
<td>Data element types shared include name, social security, DOB, mailing address, zip code, phone number and email address of Veterans being monitored by FCMT.</td>
<td>VADIR-FCMT IS A MOU v1.8 Additional notice is provided by the system’s System of Record Notice (SORN) VA (138VA005Q/74 FR 3709)</td>
<td>Electronically transferred through secured connection using Http (Hypertext Transfer Protocol)</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Virtual Lifetime Electronic Record (VLER) Data Access Service (DAS)</td>
<td>DoD Case Management System (DoD-CMS) being monitored by FCMT used to monitor, track and create SM/V client records</td>
<td>VLER DAS shares all data types such as Name, date of birth (DOB), gender, address, phone number, e-mail, SSN.</td>
<td>VADIR-FCMT IS A MOU v1.8 Additional notice is provided by the system’s System of Record Notice (SORN) VA (138VA005Q/74 FR 3709)</td>
<td>SOAP (Simple Object Access Protocol) using Hypertext Transfer Protocol Secure (HTTPS)</td>
</tr>
</tbody>
</table>

**If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.**

Physical Security: Access to data processing centers is generally restricted to center employees, custodial personnel, Federal Protective Service and other security personnel. Access to computer rooms is restricted to authorized operational personnel through electronic passage technology. All other persons needing access to computer rooms are escorted. Information physically transported outside of the agency’s perimeter, including information transported on removable media and portable mobile devices are first requested by the individual utilizing the devices. Once approved by management as well as information security, the device is tracked by an assigned identifying number and barcode and secured by PKI encryption.

System Security: Access to the VA network is protected by the usage of “logon” identifications and passwords. Once on the VA network, separate ID and password credentials are required to gain access to the FCMT server and/or database. Access to the server and/or database is granted to only a limited number of system administrators and database administrators. Users of FCMT access the system via the approved VA Trusted Internet Connection or through the VA's Virtual Private Network. Users must have accounts in the VA's Active Directory (AD) system. Upon
approval of a VA AD account, they may request access to FCMT. Within the FCMT system, users are designated a role which determines their access to specific data.

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: There is a risk that information may be shared with an unauthorized program, system, or individual.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization, 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 are all measures that are utilized within the facilities. VA will transfer data to DoD through secure file transfer protocol (FTP), encrypted or password protected physical storage media, or other appropriately secure means, personally identifiable information (PII) and protected health information (PHI) maintained by VA (VA data) in accordance with cited references as they are requested by DoD and/or they become available as subsequent to the request.

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.

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, 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 https://www.govinfo.gov/content/pkg/FR-2009-07-27/pdf/E9-17776.pdf

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).

6.2 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?

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

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.

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?

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.

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.

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, MVI).

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 (VADIR, MVI).

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, MVI) 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. 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 ensure data accuracy.
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 individual’s 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, MVI) 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.

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?

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.
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.

**Developer Access:**
Developers account management processes should further ensure that only end-users are able to access the environment. Developers and FCMT Project teams will work to create, update, access and disable developer 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 POC is the only person who may submit account creation requests and submitted for accountability purposes.

**End-user and Tester Access:**
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 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 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 developer, 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 requests 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.

8.2 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 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?

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. 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.

FCMT was covered under the Customer Relations Management (CRM) ATO however when that ATO was transitioned it fell under BAM CRM ATO which is available until December 2020. The FIPS 199 classification of the system is Moderate. FCMT is in the process of creating an
individual ATO specifically for this application. A&A is in progress and IOC date of 12/20/2020.
### Section 9. References

**Summary of Privacy Controls by Family**

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

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

RITA K GREWAL
114938
Digitally signed by RITA K GREWAL 114938
Date: 2020.08.19 15:50:56 -04'00'

Privacy Officer, Rita Grewal

Roland B Parten
596219
Digitally signed by Roland B Parten 596219
Date: 2020.08.19 12:42:57 -05'00'

Information Security Systems Officer, Roland Parten

Paul T. Zeien
264273
Digitally signed by Paul T. Zeien 264273
Date: 2020.08.19 13:27:15 -05'00'

Information System Owner, Paul T. Zeien
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).