



Privacy Impact Assessment for the VA IT System called:

Data Migration and Management (DMM) Electronic Health Records Modernization VA Central Office

Date PIA submitted for review:

2/13/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov	202-632-8431
Information System Security Officer (ISSO)	Jeremy Drake	Jeremy.drake@va.gov	509-956-8865
Information System Owner	Augie Turano	Augie.turano@va.gov	412-241-0217

Abstract

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

The DMM (VistA eXtract of 130 VAMCs) mechanism funnels the data from all VistA nationwide systems to the Veterans Health Administration (VHA) Data Migration and Management (DMM). The DMM utility is designed to allow for full extraction of VistA data from specific sites or to aggregate data at Veterans Integrated Service Network (VISN), Regional, or National levels.

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. The IT system name and the name of the program office that owns the IT system.*

Data Migration and Management (DMM) VA Central Office (VACO)

- B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*

The DMM system houses a mirror copy of 25 million individual Veterans medical records. The system contains PII and PHI data and is collected for the Electronic Health Records Management systems of the Veterans Administration and Department of Defense. The Data Migration and Management system sends data to Cerner for integration into the HealthIntent Department of Defense Electronic Health Record (EHR) system and also populates the Corporate Data Warehouse.

- C. Indicate the ownership or control of the IT system or project.*

Veterans Administration Owned and Operated

2. Information Collection and Sharing

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

25 million. Veterans currently or previously in the care of the Veterans Health Administration

- E. A general description of the information in the IT system and the purpose for collecting this information.*

Data Migration and Management VA VistA data is transmitted to a mirror DMM in the Cerner data center for consumption by HealthIntent and Millennium, components of the new VA Electronic Health Record Modernization (EHRM). Data syndication is capturing the

returning data from Cerner Millennium EHR and merging it with other VA data to be used for reporting and analytic platforms.

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

The system operates out of the Austin Information Technology Center, there are also mirrored systems based at Cerner and in Microsoft Azure Government. The systems maintain a duplicate of the onsite databases at the remote sites. The data is encrypted in transit and at rest at all sites

G. 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.

The system operates out of the Austin Information Technology Center, there are also mirrored systems based at Cerner and in Microsoft Azure Government. The systems maintain a duplicate of the onsite databases at the remote sites. The data is encrypted in transit and at rest at all sites

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

The legal authority to operate falls under Title 38, United States Code, section 7301(a).

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?

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/202028340.pdf>. The SORN will not require amendment or revision.

D. System Changes

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

The PIA will not result in circumstances that require changes to business processes

K. Whether the completion of this PIA could potentially result in technology changes
No technology changes required

Section 1. Characterization of the Information

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

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

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

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

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

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

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

PII Mapping of Components (Servers/Database)

Data Migration and Management consists of 21 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Data Migration and Management 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 the server names in the table. *The first table of 3.9 in the PTA should be used to answer this question.*

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
FDW1 B1930 BISL_MILL ODS SSISDB CSDE_BSV DDSCClient LSV OEHRM OMHSP_PERC PBM_CERNER RSConversionResults SPV DSYNB3 DSYNImport ETL LDW SDW DMMCore ERWinModelMart ValueXWalk	Yes	Yes	Name, SSN, DOB, Mothers maiden name, personal mailing address, zip code, personal phone number, personal fax number, personal email address, contact information, next of kin, emergency contact information, health insurance, certificate/License numbers, medications, medical records, race/ethnicity, medical record number, gender	The DMM utility is designed to allow for full extraction of VistA data from specific sites or to aggregate data at Veterans Integrated Service Network (VISN), Regional, or National levels. The DMM method involves reading journal files, pattern matching particular data fields of interest, and then migrating the identified fields to the DMM system. The DMM system uses InterSystems Cache mirrors and multiple journal readers.	Access to the system is restricted and access to specific information is limited to need to know.

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 DMM data are the VistA production databases via the VistA Shadow server process.

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

The primary sources of DMM data are the VistA production databases via the VistA Shadow server process.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

The system does not create 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?

DMM collects data from the VistA Shadow Servers. This data is transferred to DMM via the Enterprise Connection Protocol (ECP).

1.3b 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.

DMM does not use a form in the collection 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.

The DMM implements data integrity checking using InterSystems IRIS software to check data to ensure VistA data reflects the values stored in the source systems. DMM Data Quality (DQ)

tools are used on a daily basis to compare the data between a site's VistA Shadow and the DMM databases, fix unreconciled records, and report anomalies so that they can be addressed.

1.4b 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.

The DMM implements data integrity checking using InterSystems Datacheck to ensure VistA data reflects the values stored in the source systems. DMM Data Quality (DQ) tools are used on a daily basis to compare the data between a site's VistA Shadow and the DMM databases, fix unreconciled records, and report anomalies so that they can be addressed. The Data Quality checks are run using Docker containers that create an ECP connection to a VistA shadow site and to the DMM mirror. The DQ check is run in a VA Docker container. The containers are managed using Portainer which is an open-source container management tool that works with the Docker Platform.

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

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

Title 38, United States Code, section 7301(a). 38 U.S. Code § 7301 - Functions of Veterans Health Administration: in general

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: The Privacy risk may occur when the data may become corrupted or incorrect.

Mitigation: We run routine Datacheck and integrity checks against all our databases. DMM storage is encrypted at the hardware level at both the AITC, Cerner and Microsoft Azure Government locations. In addition, all mirror traffic is encrypted in transit.

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.

DMM extracts data from all Vista instances and moves it quickly and continuously into the CDW (Corporate Data Warehouse) and Cerner's HealthIntent data platform, keeping the data from all 130 VistA EHR instances synchronized to the Cerner Data Cerner for later ingestion into Cerner's EHR (Millennium). This data is used to support health care operations. DMM forms an enterprise data platform upon which many activities can be built., including (but not limited to) APIs, applications, dashboards, and reports generated from database queries. The data in the combined repository is then available for use by data analysts, researchers, and others in the cloud.

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.

DMM uses many different application software to process the data for ingestion into Cerner. This includes InterSystems IRIS, Ensemble, and SQL. Once the data is in Caché/IRIS class form, DMM can output it in a variety of formats, including XML, JSON, text or CSV. With the support of Open Database Connectivity (ODBC) / Java Database Connectivity (JDBC), the data output by DMM is available for querying and reporting by hundreds of common tools. These

Version Date: October 1, 2022

Page 8 of 28

connections also enable data to be transformed into specific healthcare formats (such as HL7, FHIR, and X13) using InterSystems Ensemble/HealthShare/Health Connect.

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 system does not generate newly derived information

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 DMM data is encrypted at rest and in transit using SHA-256 Encryption.

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

All DMM data is encrypted at rest and in transmission while replicating to the mirrors, using TLS 1.2. For data at rest, DMM uses infrastructure encryption using platform-managed keys, as well as MACsec and hardware security devices as it traverses the TIC. Access to DMM data is determined by views so that only authorized users can see certain data elements and users must be approved by National Data Systems (NDS)

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

Primary systems are located at the Austin Information Technology Center, which is a secure facility requiring a background check for access. Systems in Azure are in the GovCloud environment. All personnel with access to the data must complete the Rules of Behavior training, the Privacy and HIPAA Training, and must also submit an elevated privileges access request for the systems which must be approved by the System Owner.

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?

DMM uses VA Active Directory user provisioning process to provide access to our systems. Any user requiring access must submit an elevated privileges request that must be approved by the System Owner.

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

Yes, criteria, procedures, controls, and responsibilities regarding access are documented in the DMM Account Management SOP document maintained on our File server share.

2.4c Does access require manager approval?

Access does require manager approval

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

The system tracks and records the access to the application which contains PII data.

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

The System Owner is responsible for assuring safeguards for the PII.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

All data loaded in DMM is retained and stored at Cerner, AITC and in Microsoft Azure Government environments. Data elements are Name, SSN, DOB, Mothers maiden name, personal mailing address, zip code, personal phone number, personal fax number, personal email address, contact information, next of kin, emergency contact information, health insurance, certificate/License numbers, current medications, previous medical records, race/ethnicity, medical record number, gender

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.** The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Records are maintained in accordance with VHA RCS 10-1 section 1100.38. Unscheduled VISTA associated records needed to perform various business duties. Retained indefinitely.

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. 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?

Yes

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

DMM uses VHA RCS 10-1 section 1100.38.VHA Records Control Schedule 10-1:
<https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf>

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.

Records are maintained in accordance with VHA RCS 10-1 section 1100.38. Unscheduled VISTA associated records needed to perform various business duties. Retained indefinitely. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal

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

https://www.va.gov/vapubs/search_action.cfm?dType=1

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.

For research, testing and training use, data remains hosted on encrypted storage arrays, which limit access unless personnel are given specific permissions which must be approved by the System Owner.

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: Data may be exposed when retained beyond what is necessary.

Mitigation: These measures include access control, awareness and training, audit and accountability, certification, accreditation, and security assessments, configuration management, contingency planning,

Version Date: October 1, 2022

Page 12 of 28

identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and system and information integrity.

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

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
Data and Analytics/Corporate Data Warehouse	The DMM (VistA eXtract of 130 VAMCs) mechanism funnels the data from all VistA nationwide systems to the Veterans Health	Name, SSN, DOB, Mothers maiden name, personal mailing address, zip code, personal phone number, personal fax number, personal email address, contact information, next of	SQL Database Replication from IRIS to SQL

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
	Administration (VHA) Corporate Data Warehouse (CDW). The DMM utility is designed to allow for full extraction of VistA data from specific sites or to aggregate data at Veterans Integrated Service Network (VISN), Regional, or National levels.	kin, emergency contact information, health insurance, certificate/License numbers, current medications, previous medical records, race/ethnicity, medical record number, gender	
Veteran’s Health Administration (VHA)/VistA	The DMM (VistA eXtract of 130 VAMCs) mechanism funnels the data from all VistA nationwide systems to the Veterans Health Administration (VHA) Corporate Data Warehouse (CDW). The DMM utility is designed to allow for full extraction of VistA data from specific sites or to aggregate data at Veterans Integrated Service Network (VISN), Regional, or National levels.	Name, SSN, DOB, Mothers maiden name, personal mailing address, zip code, personal phone number, personal fax number, personal email address, contact information, next of kin, emergency contact information, health insurance, certificate/License numbers, current medications, previous medical records, race/ethnicity, medical record number, gender	IRIS Enterprise Cache Protocol (ECP)

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: Risk of access and misuse of information by a VA employee

Mitigation: All systems receiving data from DMM on VA systems are subject to VA security and privacy controls managing data. Active directory is used for access controls and resources are given access to only the systems needed to perform their duties. We also monitor system access through logs and scans

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

<p>List External Program Office or IT System information is shared/received with</p>	<p>List the purpose of information being shared / received / transmitted with the specified program office or IT system</p>	<p>List the specific PII/PHI data elements that are processed (shared/received/transmitted) within the Program or IT system</p>	<p>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</p>	<p>List the method of transmission and the measures in place to secure data</p>
<p>Cerner/DoD</p>	<p>The DMM system houses a mirror copy of 25 million individual Veterans medical records. The system contains PII and PHI data and is collected for the Electronic Health Records Management systems of the Veterans Administration and Department of Defense. The Data Migration and Management system sends data to Cerner for integration into the HealthIntent Department of Defense EHR</p>	<p>Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, next of kin, emergency contact information, health insurance, certificate/License numbers, current medications, previous medical records, race/ethnicity, medical record number, gender</p>	<p>National ISA/ MOU</p>	<p>IRIS Mirroring (Site to Site (S2S), Secure FTP. Data is encrypted at rest and in transit for all interconnections</p>

	system and also populates the Corporate Data Warehouse			
--	--	--	--	--

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: Risk of sharing more data than is appropriate.

Mitigation: There are contracts, business associate agreements, and MOUs that outline how VA data must be protected, used, and destroyed when the use has ended

The risk of sharing more data than appropriate is highly unlikely, all the data we collect from VistA is transferred to CDW and Cerner\DOD. Connectivity to our environment requires an approved certificate and authentication. We are currently in the process of renewing our MOU to reflect the status of DMM as a major application.

Section 6. Notice

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

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

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the

Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

This system transfers data within the VA network, therefore Notices are provided at the point of collection, medical provider, VA Medical Center. All Veterans received a Notice of Privacy Practices (NOPP) every 3 years, link provided in appendix A.

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

Notice is not directly provided by this system, but the SORN provides notice as well as the NOPP.

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf> (govinfo.gov) Per the SORN: Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

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.

This system transfers data within the VA network, therefore Notices are provided at the point of collection, medical provider, VA Medical Center. All Veterans received a Notice of Privacy Practices (NOPP) every 3 years, link provided in appendix A.

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf> (govinfo.gov) Per the SORN: Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

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.

This system transfers data within the VA network, therefore Notices are provided at the point of collection, medical provider, VA Medical Center.

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.

This system transfers data within the VA network, therefore Notices are provided at the point of collection, medical provider, VA Medical Center.

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: Individuals might not know how data in DMM may be used, collected or disclosed.

Mitigation: For Veterans receiving health care by VHA, each receives a Privacy Notice every 3 years. In addition, the System of Record Notice is published in the Federal Register explaining the categories of records stored in the system and routine uses of the data.

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.

This system transfers data within the VA network, therefore Notices are provided at the point of collection, medical provider, VA Medical Center. The VA SORN addressed records correction in VistA System.

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

The system is not exempt from the access provisions 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.

DMM is a privacy act system that contains VA data including PII and PHI.

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.

This system transfers data within the VA network, therefore Notices are provided at the point of collection, medical provider, VA Medical Center. The VA SORN addressed records correction in VistA System. A link to the NOPP is provided in appendix A.

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.

This system transfers data within the VA network, therefore Notices are provided at the point of collection, medical provider, VA Medical Center. The VA SORN addressed records correction in VistA System. A link to the NOPP is provided in appendix A.

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 ensure data accuracy.***

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

This system transfers data within the VA network, therefore Notices are provided at the point of collection, medical provider, VA Medical Center. The VA SORN addressed records correction in VistA System. A link to the NOPP is provided in appendix A.

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: Individuals are not aware of what is being collected in the Data and Migration Management System.

Mitigation: The VA SORN addressed records correction in VistA System, this PIA also serves as a notice to the public about data collection, use and disclosure.

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.

All requests for data access are managed through the ePAS system where each request and approval are recorded. For local or VISN level access, a similar process is in place for granting a user access to one or more VHA facilities data.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Other agencies do not have access to the system

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.

Users granted privileged level access via ePAS requests have access to the system. These users must complete the training required for their access in TMS. IT Software Developers - Information Security Role-Based Training for IT Specialist, Data Managers, Network Administrators - Information Security and Privacy Role-Based Training for Network Administrators, System Administrators - Information Security Role-Based Training for System Administrators

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors are required to take Privacy and Security training to have a PIV card and a VA network account. All contractors requiring data Access must sign the VA Non-disclosure agreement.

The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors are required to take Privacy and Security training to have a PIV card and a VA network account. Contractors are required to apply for DMM data access through ePAS for elevated privileges with the approval of the supervisor and the Contracting Officer Representative must approve the contractor's access to DMM.

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.

All users with access to VA sensitive information or information system must complete VA Privacy and Security Awareness Rules of Behavior Training (TMS#10176) initially and annually thereafter. Additionally, if users will be accessing protected health information (PHI) data VA HIPAA Privacy training (TMS#10203) is required initially and annually thereafter

IT Software Developers - Information Security Role-Based Training for IT Specialist, Network Administrators - Information Security and Privacy Role-Based Training for Network Administrators, System Administrators - Information Security Role-Based Training for System Administrators

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 10/19/2022
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 11/28/2022
5. *The Authorization Termination Date:* 05/27/2023
6. *The Risk Review Completion Date:* 11/25/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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.***

Please provide response 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 (ITMAaaS). 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)

DMM is primarily hosted on premise at the VA Austin Information Technology Center. DMM also supports a copy of its data in the VA Enterprise Cloud provided by Microsoft Azure Government (MAG). Infrastructure as a service (IaaS) and Platform as a Service (PaaS) are both currently being utilized.

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.*

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.

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.

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

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

DMM is not using RPA

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

Privacy Officer, Julie Drake

Information Systems Security Officer, Jeramy Drake

Information Systems Owner, Augie Turano

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).

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

Veteran Health Administration Notice of Privacy Practices (September 30, 2022) You may also obtain a copy of this Notice at the following website: <http://www.va.gov/vhapublications>.

Under Brochures:

10-163P	VA Notice of Privacy Practices , 105HIG - Health Information Governance	09/30/2022	
---------	---	------------	--

HELPFUL LINKS:

Record Control Schedules:

<https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf>

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

<https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf>

National Archives (Federal Records Management):

<https://www.archives.gov/records-mgmt/grs>

VHA Publications:

<https://www.va.gov/vhapublications/publications.cfm?Pub=2>

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](#)