Privacy Impact Assessment for the VA IT System called:

Financial Data and Masking Extract Transform Load

Veterans Affairs Central Office (VACO)

Financial Technology Service

Date PIA submitted for review:

8/17/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Mark A. Wilson*	*Mark.Wilson@va.gov*	*512-386-2246*
Information System Security Officer (ISSO)	*Rito-Anthony Brisbane*	*Rito-Anthony.Brisbane@va.gov*	*512-460-5081*
Information System Owner	*Jonathan Lindow*	*Jonathan.Lindow@va.gov*	*512-981-4871*

Abstract

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

Financial Data and Masking Extract Transform Load (F&M ETL) is comprised of two modules: 1. Power Center which is an Extract, Transform, and Load (ETL) utility used to build enterprise data warehouses, 2. Test Data Management (TDM) module which provides the ability to de-identify data as well as view and analyze business information and browse and analyze metadata from disparate metadata repositories. This technology allows development teams to extract data from multiple sources, transform the data according to business logic developed in the client application, load the transformed data into a file and relational targets, and/or de-identify PII/PHI data.

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.*

System Name: FINANCIAL DATA AND MASKING EXTRACT TRANSFORM LOAD (F&M_ETL); Program Office: FINANCIAL TECHNOLOGY SERVICE

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

F&M ETL is used to integrate claims & payment data for reporting. Information is used for forecasting, budgeting, and audit. The system is also used as a means of making de-identified data available to all FSC Product Lines in lower environments for testing by product development teams to ensure no production data is in those lower environments.

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

Ownership and control of the F&M ETL systems falls under Financial Service Center (FSC) Financial Technology Service (FTS).

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.*

The F&M ETL system does not collect, store, or share any PII or PHI information for any individual. The system is comprised of two modules 1. Power Center which is an Extract, Transform, and Load (ETL) utility used to build enterprise data warehouses, 2. Test Data Management (TDM) module which provides the ability to de-identify data. This technology allows development teams to extract data from multiple sources, transform the data according to business logic developed in the client application, load the integrated data into relational targets where PHI and PII is de-identified.

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

The ETL portion of the system is used to integrate claims & payment data for reporting. No PII or PHI information is contained within this process. Process description as follows - Extract: Data is pulled from various claims and payment source systems. Transform: Claims and Payment data is matched to the FMS general ledger. Load: Matched data populates the Payment Data Repository (PDR). The TDM portion of the system reads production data and then de-identifies that data for use in lower environments for FSC product teams to use for development and test. This provides them production quality de-identified data in lower environments. No PII is collected or stored in this process.

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

The F&M ETL system consumes data from claims and payment data source systems. After performing internal transformation functions within the F&M ETL system data is then passed to the FSC Data Depot. Claims and Payment data go to the Payment Data Repository (PDR) whereas de-identified data is passed to the Data Depot lower environments. In either case no PII or PHI is passed out from the F&M ETL system.

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 F&M ETL system is an internal tool within the FSC to provide services to its customers. The system is used solely by the F&M ETL development team at the FSC only.

3. Legal Authority and SORN

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317. The F&M ETL system received its Authority to Operate (ATO) on 11 April 2023.

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?*

No SORN is required for this system.

D. System Changes

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

All existing business processes in place will remain the same and no new business processes will be required.

K. *Whether the completion of this PIA could potentially result in technology changes*

No required technology changes have been identified.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Veteran ID, Vendor ID/Patient ID/Member ID, ZIP Code, Ethnic Group ID, Accident State, Federal Tax ID Type, Diagnosis Code, Procedure Code, Date of Death, Patient SSN, Patient Zip Code

PII Mapping of Components (Servers/Database)

The Financial Data and Masking Extract Transform Load (F&M ETL) system consists of four key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by F&M_ETL 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.

Internal Database Connections

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
Claims History	Yes	No	Vendor ID	Data De-Identification	Once the data is De-Identified, the data is no longer PII
Payment History	Yes	No	Vendor ID	Data De-Identification	Once the data is De-Identified, the data is no longer PII
Community Care	Yes	No	Patient Birth Date, Patient First Name, Patient Gender, Patient Last Name, Patient SSN, Patient Zip Code	Data De-Identification	Once the data is De-Identified, the data is no longer PII
Claims Management	Yes	No	Member First Name, Member Last Name, Ethnic Group ID, Gender,	Data De-Identification	Once the data is De-Identified, the data is no longer PII

			Accident State, Zip Code, Vendor ID, Federal Tax ID, Federal Tax ID Type		

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?

F&M_ETL collects information from FSC systems and the Financial Management System (FMS).

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.

F&M_ETL transforms all data collected for the purposes of making data available for claims and payment reporting or for de-identifying data for FSC products to use during testing.

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

F&M_ETL loads the data into the IBNR_OCC database for claims and payment data reporting and to the Data Depot test environment to make the de-identified data available to all FSC products requiring data to test with.

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?

All data collected by F&M_ETL is received from existing VA databases by creating connections with an authorized account. F&M_ETL transforms data based on business requirements. The data is read from provisioned accounts. Credentials for provisioned accounts are approved by the source data owners. Access and authorization to the data read by F&M_ETL is controlled through a given account by a provisioned account for access to a specific set of tables based on approval provided. That provisioned account is then used by F&M_ETL to make the connection to the database. All PII and PHI data is de-identified before populating the target database.

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.

Data is not collected on a form.

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.

F&M_ETL is processing data and not storing it. Responsibility for the accuracy of the information is the F&M_ETL Development Team responsibility. Currently the F&M_ETL Team has a series of reports for Audit and Accuracy validation which runs monthly. For Data De-identification this is not applicable. The data from the source is simply de-identified and placed in lower environments. F&M_ETL is not used making any decisions about individuals.

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 system does not use a commercial aggregator.

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317. Legal authority does not apply as F&M_ETL is used as a tool to enable better privacy compliance for all FSC Products and Applications. Production quality test data will be loaded in lower environments to ensure that no production data is used for development or testing.

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 risk for disclosing any private information is very low. Firewall rules are applied to allow the data to flow from the source database to F&M_ETL Secure connections (SSL – Secure Socket Layer) are made at the database level. All data collected by F&M_ETL goes through goes through Random Access Memory (RAM) which is overwritten as it is consumed by the F&M_ETL Tool. No Privacy data is stored in F&M_ETL.

Mitigation: The access to F&M_ETL is controlled by Active Directory Authentication mechanisms. Authorization is controlled by the F&M_ETL Admin based on role. F&M_ETL is the tool that is used to mitigate the disclosure of privacy data. All data moved to the target database is de-identified.

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.

F&M_ETL is currently used for two purposes 1) Collecting and integrating Payment and Claims data into a central database and 2) Data De-Identification. The business purpose for Payment and Claims data is for audit and reporting Purposes. No PII or PHI is collected or used for Payment and Claims data. The business purpose for Data De-Identification is to ensure that no PII or PHI is used in lower environments for development or test purposes. The following PII and PHI data elements as listed in section 1.1 of this document are not used by the system nor is it made available to any users. The purpose of the tool is to read the data elements from the source production environment, de-identify the date elements, then write that de-identified data to the test environment for development and test teams for use in their development and testing processes.
Name
Social Security Number
Date of Birth
Tax Identification Number
Gender
Veteran ID
Vendor ID/Patient ID/Member ID
ZIP Code, Ethnic Group ID
Accident State
Federal Tax ID Type
Diagnosis Code
Procedure Code
Date of Death
Patient SSN
Patient Zip Co

Diagnosis Code
Procedure Code
Date of Death

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.

F&M_ETL is currently used for two purposes 1) Collecting Payment and Claims data and 2) Data De-Identification. F&M_ETL is an ETL tool used to accurately integrate large amounts of data to produce a data repository for Payment and Claims data reporting and subsequent analysis. The tool is used for transformation and load purposes. After the data is loaded into the target database external tools are used to read data from the target database for analysis. No information is available to drill down to the patient level as PII or PHI is not collected or used for Payment and Claims data. F&M_ETL is also used for Data De-identification which ensures that no production data that includes PII or PHI is available to developers or testers working on FSC Products and Applications.

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 F&M ETL system does not create or make available any new or previously unutilized information about an individual.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

Data in transit uses standard VA protocols to ensure data is protected. Firewall rules are applied to allow the data to flow from the source database to F&M_ETL Secure connections (SSL – Secure Socket Layer) are made at the database level. Data is encrypted in flight and no data is at rest within the F&M_ETL Tool. Access and authorization to the data read by F&M_ETL is controlled through a given account by a provisioned account for access to a specific set of tables based on approval provided. That provisioned account is then used by F&M_ETL to make the connection to the database secured by Kerberos. (Note - Kerberos is used for SQL Server connections and Oracle connections are secured by internal F&M_ETL controls.)

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

SSNs are de-identified using F&M_ETL processes for data masking. There is a governance process in place to gain access to the F&M_ETL Tool. There are also service accounts as security controls to limit access to databases to F&M_ETL product only. Users that required access are provided by security protocols and governance. Permanent and consistent masking of sensitive data including SSN and masking cannot be reversed.

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

The F&M ETL system does not store PII/PHI. Once the PII/PHI is read it is immediately de-identified.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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

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

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

<u>Principle of Use Limitation:</u> 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?

User access and authorization is controlled through standard security process and approvals for database access. Leveraging standard FSC approval processes through submission of 9957 requests which include manager approvals. Additionally, there are standard monitoring processes in place to drop access when a user leaves the VA.

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

All procedures, controls and responsibilities are documented within the FSC FTS.

2.4c Does access require manager approval?

Approval processes are controlled through the 9957 submissions for manager approval.

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

Access is monitored, tracked, and recorded through 9957 submissions.

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

The system owner assures all processes and procedures are followed.

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*

No business data is retained within the F&M_ETL Tool. Only Metadata is retained in F&M_ETL Metadata is defined as Internal F&M_ETL information (source code and settings & configuration information). Metadata is defined as field names, no actual data within the fields are retained. All data retention is in the target database which will not contain PII or PHI data.

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.*

N/A – No information is retained.

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?

N/A – No information is retained.

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

N/A – No information is retained.

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.

N/A – No information is retained. No physical records exist.

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.

F&M_ETL is a tool that eliminates the need to use production PII and PHI data for development and or testing.

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: N/A – No information is retained.

Mitigation: N/A – No information is retained.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Claims History	Data De-Identification	Vendor ID	SSL-Secure Socket Layer
Payment History	Data De-Identification	Vendor ID	SSL-Secure Socket Layer
Community Care	Data De-Identification	Patient Birth Date Patient First Name Patient Gender Patient Last Name Patient SSN Patient Zip Code	SSL-Secure Socket Layer
Claims Management	Data De-Identification	Member First Name Member Last Name Ethnic Group ID Gender Accident State Zip Code Vendor ID Federal Tax ID Federal Tax ID Type	SSL-Secure Socket Layer

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: User access and authorization is controlled through standard security process and approvals for database access.

Mitigation: Leveraging standard FSC approval processes through submission of 9957 requests which include manager approvals. Additionally, there are standard monitoring processes in place to drop access when a user leaves the VA. No front-end users have access to this system. There are less than 10 backend users that have access to this system.
Both contractor and VA are required to take Privacy, HIPAA, and information security training annually.

- Information is shared in accordance with VA Handbook 6500
- File access granted only to those with a valid need to know

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a

Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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:

<u>Privacy Risk:</u> N/A – No external data is shared or received.

<u>Mitigation:</u> N/A – No external data is shared or received.

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.

F&M_ETL does not collect information from individuals. F&M_ETL is a tool for movement and integration of data that has already been collected.

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

F&M_ETL does not collect information from individuals. F&M_ETL is a tool for movement and integration of data that has already been collected.

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.

F&M_ETL does not collect information from individuals. F&M_ETL is a tool for movement and integration of data that has already been collected.

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.

F&M_ETL does not collect information from individuals. F&M_ETL is a tool for movement and integration of data that has already been collected. This falls under the responsibility of the system collecting the information.

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.

N/A – F&M_ETL does not collect information from individuals. F&M_ETL is a tool for movement and integration of data that has already been collected.

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: N/A – F&M_ETL is a tool for movement and integration of data that has already been collected.

Mitigation: N/A – F&M_ETL is a tool for movement and integration of data that has already been collected.

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.***

The source systems are responsible for collection of information from individuals. F&M_ETL does not collect information from any individuals. F&M_ETL is a tool for movement and integration of data that has already been collected.

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).

F&M_ETL does not collect information from individuals. F&M_ETL is a tool for movement and integration of data that has already been collected.

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.

F&M_ETL does not collect information from individuals. F&M_ETL is a tool for movement and integration of data that has already been collected.

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.

N/A – The source systems are responsible for collection of information from individuals. F&M_ETL does not collect information from individuals. F&M_ETL is a tool for movement and integration of data that has already been collected.

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 source systems are responsible for collection of information from individuals. F&M_ETL does not collect information from individuals. F&M_ETL is a tool for movement and integration of data that has already been collected.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The source systems are responsible for collection of information from individuals. F&M_ETL does not collect information from individuals. F&M_ETL is a tool for movement and integration of data that has already been collected.

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: N/A – F&M_ETL does not collect information from individuals. F&M_ETL is a tool for movement and integration of data that has already been collected.

Mitigation: N/A – F&M_ETL does not collect information from individuals. F&M_ETL is a tool for movement and integration of data that has already been collected.

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.

User access and authorization is controlled through standard security process and approvals for database access. Leveraging standard FSC approval processes through submission of 9957 requests which include manager approvals. Additionally, there are standard monitoring processes in place to drop access when a user leaves the VA. Identity management in F&M_ETL is dependent on the VA's Windows Active Directory (AD) for authentication. Users must complete and submit a 9957 form for access to F&M_ETL. The submitting individual's manager must approve the 9957 for the 9957 to reach the System Administrator's queue for processing. The user must be in a designated security group and if a user is not in the appropriate security group, he or she will not be able to access the application.

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?

No users from other agencies have access to this 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 of the F&M ETL system are developers only and only have read-only access to the data on source systems feeding the F&M ETL system.

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

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

Yes, contractors do have access. Contractors have responsibility for maintaining the F&M_ETL system. All contractors have completed background checks and normal FSC on-boarding Version Date: October 1, 2022 Page 23 of 30 procedures. NDAs are signed and "Privacy and Information Security Awareness and Rules of Behavior" training is conducted annually. Development teams consist of contractors for both System Administrators and Developers. Roles have been established and separated out between Developers and Administrators for appropriate access within the F&M_ETL tool. All roles are contained in the SOP.

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.

"Privacy and Information Security Awareness and Rules of Behavior" training is conducted annually.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved/ Yes
2. *The System Security Plan Status Date:* SSP signed on 10-26-2022
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 11 July 2022
5. *The Authorization Termination Date:* 07 January 2023
6. *The Risk Review Completion Date:* 02 June 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.***

N/A- ATO

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

F&M ETL utilizes the VAEC as described here: F&M_ETL is currently hosted on the Microsoft Azure for Government (MAG) Cloud. The F&M_ETL platform with its TDM and PowerCenter components are FedRAMP authorized. F&M_ETL product is COTS, PaaS to provide data integration and data masking services.

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.*

No, F&M_ETL will be hosted on VA Enterprise Cloud Microsoft Azure Government (MAG).

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

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

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

No. F&M_ETL will be hosted on VA Enterprise Cloud Microsoft Azure Government (MAG).

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.

Not applicable. F&M_ETL is hosted on the VA Enterprise Cloud Microsoft Azure Government (MAG), and the ATO for MAG covers this principle of security and privacy.

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).

RPA is not used.

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

ID	Privacy Controls
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

MARK WILSON Digitally signed by MARK WILSON
Date: 2023.10.19 12:14:40 -05'00'

Privacy Officer, Mark A. Wilson

RITO-ANTHONY BRISBANE Digitally signed by RITO-ANTHONY BRISBANE
Date: 2023.10.19 12:31:42 -05'00'

Information System Security Officer, Rito-Anthony Brisbane

JONATHAN LINDOW Digitally signed by JONATHAN LINDOW
Date: 2023.10.19 13:27:26 -05'00'

Information System Owner, Jonathan Lindow

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).

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