Privacy Impact Assessment for the VA IT System called:

MARi

VA Corporate (VACO)

ILEAD

Date PIA submitted for review:

09/15/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jacqueline Levett	Jacqueline.Levett@va.gov	909-825-7084
Information System Security Officer (ISSO)	LaWanda Wells	Lawanda.Wells@va.gov	202-632-7905
Information System Owner	Aimee Barton	Aimee.Barton@va.gov	216-707-7726

Abstract

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

MARi is a Learning Record Store (LRS) that will be used to collect and report on key specialized data via the Application Programming Interface (API) standard, such as time spent on individual online learning activities, sub scores, competency proficiency, etc. All elements of the solution must be available outside the firewall, as some staff may be at home when accessing courses, similarly to the existent Talent Management System (TMS).

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.

The MARi system is a Learning Record Store (LRS) Software as a Service (SaaS) that will be controlled by the ILEAD program office.

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

This system will be an enterprise solution and is meant to continue advancing training for VHA employees across the enterprise by supporting custom-designed digital learning experiences via the Application Programming Interface (API) standard.

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

The system is owned and operated by the providing SaaS vendor and will be controlled by the ILEAD program office.

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.

This system is expected to store the information of all VA, VHA, NCA, and VBA employees, currently estimated to be approximately 400,000 people.

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

This system will collect performance relevant information about users such as name, contact information, role, etc. as well as course and assessment related information, such as performance and

time spent on each activity. The primary purpose of all information collected, created and/or stored is for the service of customized adaptive learning by producing analytics from the information collected.

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

There are currently no plans for any information sharing conducted by the IT 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 system is a Cloud service, hosted within the FedRAMP authorized Google Services Google Cloud Platform Products (GCP), so is not operated at more than one site.

3. Legal Authority and SORN

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

Privacy Act of 1974 provides protection and release information for data. E-Government Act of 2002 requires PIA. OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 specifies agency requirements, which when met, allow the agency to collect and store necessary PII. Code of Federal Regulations Part 293, and OPM's Operating Manual, "The Guide to Personnel Recordkeeping" which provide specific guidance on the collection and use of data within the agency.

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?

This system is covered by two SORNs: OPM Government-1, General Personnel Records: 2012-29777 and 76VA05 General Personnel Records (Title 38): 00-18287. SORN 76VA05 does require an update due to age, which has been requested formally through the Privacy Service. These do cover Cloud Storage.

D. System Changes

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

The completion of this PIA is expected to result in circumstance that require changes to business processes. This system will result in a change to business application for training efforts.

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

The completion of this PIA is expected to require technology changes. This system is part of a long-term effort for overall training effort improvements, and in the future would result in technology changes.

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)

- Email (VA email address only)
- System Generated ID Number
- Unique Username
- Current Role
- Current Job

- Prior Experience
- Training History
- Location
- Years Employed by VA
- Education Level
- Certifications (Occupational, Education, Medical)
- Training Transactional Records
- Course Completion Status
- Activity Completion Status
- Course Grades/Scores
- Learning Activity Transactional Data
- Competency Proficiencies
- Aptitude Assessments
- Interest Assessments
- Personality & Motivation Assessments

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

PII Mapping of Components (Servers/Database)

MARi consists of **0** 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 **MARi** 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
N/A	N/A	N/A	N/A	N/A	N/A

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 following information will be provided by the VA Employee when entering the MARi system and then transferred into the system via .csv or other file format import on an ongoing basis as required: First Name, Last Name, Email (VA email address only), System Generated ID Number, Unique Username, Current Role, Current Job, Prior Experience, Training History, Location, Years Employed by VA, Education, and Certifications. The following analytics will be provided by the MARi system once the other data has been collected: Competency Proficiencies, Aptitude Assessments, Interest Assessments, Personality & Motivation Assessments.

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.

MARi collects and analyzes the skill proficiency of organization's members as reported by external assessments and training content to support the most effective deployment of training time and resources.

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

Learning analytics and insights from the employee input and .csv and other file format import are created in MARi and provide secondary source of information.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

The above-referenced information will be collected from the VA Employee/individual via xAPI (Application Programming Interface) statements. All collected information will be provided via electronic import via .csv or other file import. The listed analytics data will be collected by the MARi system from the other data collected: Competency Proficiencies, Aptitude Assessments, Interest Assessments, Personality & Motivation Assessments.

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.

Information is not collected on a physical 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.

The information stored in MARi is information that has been collected from either direct input from authorized VA users or from .csv or other file format import and training content and from data created from MARi analytics. The accuracy of the direct input and .csv or other file format import is verified in those systems. MARi's analytics are verified on an as-needed basis using psychometric analysis and other verification algorithms that are continuously monitored by MARi for accuracy.

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 of information.

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

Privacy Act of 1974 provides protection and release information for data. E-Government Act of 2002 requires PIA. OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 specifies agency requirements, which when met, allow the agency to collect and store necessary PII. Code of Federal Regulations Part 293, and OPM's Operating Manual, "The Guide to Personnel Recordkeeping" which provide specific guidance on the collection and use of data within the agency.

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

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

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

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: Training data and competency proficiency information could be used for unintended purposes.

Mitigation: The information is deemed essential for the tracking and management of appropriate relevant training. Procedures, controls, and responsibilities are initially determined by the VHA, with role-based access control features in place for continued operations. Only the VHA and the individual user have access to their PII. Google Services including Google Cloud Platform Products (GCP) has been authorized by FedRAMP (FR1805751477, 11/22/2019). See Google Services FedRAMP for specific GCP mitigation entries.

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.

First Name: Used to identify user first name, Last Name: Used to identify user last name, Email (VA email address only): Used to provide contact information and communications used by VA/users, System Generated ID Number: Used for internal data correlation, Unique Username: Used to provide records management and overall security for user information, Current Role: Used to identify user current operational role in order to address training documentation and requirements, Current Job: Used to identify VA user current GS job category and level, Prior Experience: Used to identify user

prior experience in multiple job roles for past training documentation, Training History: Used to provide professional training history to aid in identification of potential future training requirements Location: Used to provide User current job location, Years Employed by VA: Used to identify the number of years a user has been employed by the VA, Education: Used to document user professional and technical training completed, Certifications: Used to identify user professional and technical certifications attained, Training Transactional Records: Used to track learner activity and completion rates, Course Completion Status: Used to track completed and in-progress user training, Activity Completion Status: Used to track completed and in-progress user training, Course Grades/Scores: Used to document user grades and scores for training completed, Learning Activity Transactional Data: Used to track completed and in-progress user training, Competency Proficiencies: Used to document the current proficiency of job-related competencies, Aptitude Assessments: Used to document user aptitude assessments for determining potential training Interest Assessments: Used to document individual user interests for determining prospective user training, Personality & Motivation Assessments: Used to identify individual user personality and motivational assessments for determining prospective user training

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.

MARi analyzes training and skill competency data to provide predictive and prescriptive recommendations to the organization to improve training and desired organizational outcomes. MARi conducts "match, gap, recommend" analytics. The platform a) "matches" the provided training and proficiency data to the competency requirements of the skill, b) provides a visual "gap" analysis of the delta between current and required proficiency, and c) "recommends" organization-authorized learning activities to close any gaps. The data created in the analysis is displayed in the form of visualizations to provide guidance to the organization and the individual.

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 analytics created by the system will be used to improve the overall training of the organization. The information will be used by ILEAD to train current and new VA employees more efficiently. The information would be used by ILEAD leadership to maximize the outcomes of training resources

and employee time dedicated to training. The analytics will be kept separate of a user's file and will be accessed and assessed by the Measurements Evaluation Unit (MEU). No actions will be taken against or for an individual. The analytics are used to improve the system and overall training objectives, rather than individual performance.

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 is encrypted in transit using TLS 1.2 and 1.3, and at rest using a FIPS-140-2 validated encryption module called BoringCrypto Cert #3318.

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

MARI does not collect, process or retain SSNs.

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

All data is encrypted at rest and in transit. No external information systems are used to analyze data. Additionally, GCP is FedRAMP authorized, and MARi is currently undergoing the FedRAMP process.

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?

VA manages user access and provides system overall access, including disciplinary processes for misuse of the system.

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

The PIA and SORNs clearly state that the system provides training information for VA employees. The information contained in the MARi SaaS application is relevant to the VA training mission in that it defines, manages, and tracks VA personnel training. Access to MARi is governed by Role Based Access Control, access logging and audit features provided by Google CSP. VA determines VA-internal access criteria and responsibilities within the construct of MARi user processes.

2.4c Does access require manager approval?

Yes, access requires manager approval.

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

Yes, PII access is monitored via access logs and delineates access by MARi/VA-specific roles.

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

VA is responsible for the determination of access to MARi via internal VA processes, by FedRAMP authorized GCP safeguards for overall data management, and by MARi internal process for safeguarding access and data retention.

Section 3. Retention of Information

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

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

The following information is retained by the system: First Name, Last Name, Email (VA email address only),System Generated ID Number, Unique Username, Current Role, Current Job, Prior Experience, Training History, Location, Years Employed by VA, Education, Certifications, LMS Transactional Records, Course Completion Status, Activity Completion Status, Course Grades/Scores, Learning Activity Transactional Data, Competency Proficiencies, Aptitude Assessments, Interest Assessments, Personality & Motivation Assessments.

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.*

VA training records are maintained by VA via the MARi SaaS application for the duration of user employment as directed by VA within the terms of the contract with an additional one-year retention period. Long-term records documenting individuals' Federal careers are stored in the Official Personnel Folder. This follows the requirements of OPM Government-1, General Personnel Records: 2012-29777 and 76VA05 General Personnel Records (Title 38): 00-18287, and the OPM Operational Manual "Guide to Personnel Recordkeeping (accessed Aug22, 2022 via OPM website).

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

All records stored within the system are indicated on an approved disposition authority. The contract with the vendor, MARi, outlines several provisions for records management, including the following "Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion." And "In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation."

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

The OPF is maintained for the period of the employee's service in the agency and is then the transfer and storage is in accordance with the OPM approved electronic system. Records are either retained at the agency for various lengths of time in accordance with the National Archives and Records Administration records schedules or destroyed when they have served their purpose or when the employee leaves the agency. The transfer occurs within 90 days of the individuals' separation. In the case of administrative need, a retired employee, or an employee who dies in service, the OPF is sent within 120 days. Destruction of the OPF is in accordance with General Records Schedule-1 (GRS-1).Records contained within the CPDF and EHRI (and in agency's automated personnel records) may be retained indefinitely as a basis for longitudinal work history statistical studies. After the disposition date in GRS-1 such records should not be used in making decisions concerning employees. NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a), disposition authority N1-15-06-02, item 3: 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.

MARi does not retain VA records on paper. VA records are maintained within the MARi SaaS application, which resides on the FedRAMP authorized GCP. Digital records on GCP are encrypted at rest using a FIPS-140-2 validated encryption module and destroyed by eliminating the encryption key.

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.

MARi does not use PII for research, testing, or training.

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: VA training records are maintained by VA via the MARi SaaS application for the duration of user employment as directed by VA within the terms of the VA/MARi contract.

Mitigation: VA records are maintained within the MARi SaaS application. The MARi SaaS application resides on the FedRAMP authorized Google Cloud Platform (GCP). The platform has undergone extensive analysis via the FedRAMP process. Additionally, MARi is currently in the FedRAMP authorization process at the Moderate impact level. Digital records on GCP are encrypted at rest using a FIPS-140-2 validated encryption module and destroyed by eliminating the encryption key.

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***
N/A	N/A	N/A	N/A

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: No risk is created as there is no internal sharing.

Mitigation: No mitigation is necessary as there is no Privacy Risk created.

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***
MARi	VA personnel training	First Name, Last Name, Email (VA email address only), System Generated ID Number,	76VA05 General Personnel	HTTPS:80/443 TLS 1.2 and 1.3, .csv and

	information is received directly from the VA via the MARi SaaS application, residing on the FedRAMP authorized GCP.	Unique Username, Current Role, Current Job, Prior Experience, Training History, Location, Years Employed by VA, Education, Certifications, Training Transactional Records, Course Completion Status, Activity Completion Status, Course Grade, Learning Activity Transactional Data, Aptitude Assessments, Interest Assessments, Personality & Motivation Assessments	Records (Title 38): 00-18287; OPM Government-1, General Personnel Records: 2012-29777; Contract Identifier 36C19B21C0050	flat file format imports

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: MARi shares information with the entities listed in table 5.1, which provides a data leakage risk if one of those parties are compromised.

Mitigation: Data is encrypted at rest and validated within MARi. Data sharing is initiated and configured by MARi.

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.

VA has internal privacy processes for informing VA users about collection of relevant PII for the MARi SaaS application. MARi receives VA user data directly from the VA with no MARi-generated PII user discussion. The following published SORNs also apply to Federal employees whose information is subject to the system: OPM Government-1, General Personnel Records: 2012-29777 and 76VA05 General Personnel Records (Title 38): 00-18287. SORN 76VA05. Notice regarding authorized use is also provided to internal users at sign-in of the MARi system and users acknowledge understanding.

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

Please provide response here

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.

Users acknowledge the following notice at sign-in to the MARi system: "You are accessing a system with U.S. government information. By signing an account, you acknowledge that information system usage may be monitored, recorded, and subject to audit. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties. Use of the information system indicates consent to monitoring and recording."

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.

MARi receives user data directly from VA, which provides client data according to VA internal agency discretion. A VA standard notification message will be provided at every login that provides

information related to training data right to decline, usage consent, and a link for any redress, comments, or complaints.

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.

MARi receives user data directly from VA, which provides client data according to VA internal agency discretion. A VA standard notification message will be provided at every login that provides information related to training data right to decline, usage consent, and a link for any redress, comments, or complaints.

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: VA provides user data to MARi. MARi assumes that individual users are provided Privacy notification before access.

Mitigation: The MARi SaaS application displays a notification banner at every login that states that login to va.mari.com is a United States federal government information system. It further states to the user that by signing in, you agree to only use information you have legal authority to view and use. You also agree to let us monitor and record your activity on the system and share this information with auditors or law enforcement officials. By signing in, you confirm that you understand the following: Unauthorized use of this system is prohibited and may result in criminal, civil, or administrative penalties. Unauthorized use includes gaining unauthorized data

access, changing data, harming the system or its data, or misusing the system. We can suspend or block your access to this system if we suspect any unauthorized use.

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.***

VA designates admin users with the ability to retrieve VA user information.

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

This system is not exempt.

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.

This system is a Privacy Act system.

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.

MARi receives data directly from the VA. VA manages PII data internally for accuracy and provides recourse for incorrect data. A VA standard notification message will be provided at the beginning of

every learning/training activity that will provide information related to training data right to decline, usage content, and a link for any redress, comments, or complaints.

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.

MARi receives data directly from the VA. VA manages PII data internally for accuracy and provides recourse for incorrect data. A VA standard notification message will be provided at every login that provides information related to training data right to decline, usage consent, and a link for any redress, comments, or complaints.

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.

Redress is provided.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is no risk for the MARi system specifically, as all user data is provided directly from VA.

Mitigation: Not applicable. There is no risk for the MARi system specifically, as all user data is provided directly from VA. VA provides data directly to MARi, after conducting VA-generated user access processes. VA provides a redress process exclusive of MARi operations.

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.

VA provides a list of authorized users to MARi. Users are given a temporary password which must be changed at first login.

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 other agencies have access to the MARi VA 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.

Within the MARi VA system there are two predefined roles, ADMIN and OWNER. ADMINs can access the system. OWNERs can access the system and configure their organization within the MARi 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.

VA contractors will not have access to the system or PII.

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.

VA user privacy and security training is provided by VA for VA users. MARi conducts privacy and security training to MARi internal staff.

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

8.4a If Yes, provide:

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

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.***

VA Sponsored FedRAMP ATO process is the initial A&A process for the MARi SaaS application and is In Process. The estimated IOC date is 16 APR 2024. The system is currently classified as Moderate Impact

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)*

MARi utilizes Google Services Google Cloud Platform Products (GCP) Infrastructure as a Service (IaaS) capabilities. GCP is FedRAMP authorized. MARi does not yet have FedRAMP Authorization, and it is currently in process of pursuing a VA Sponsored FedRAMP Authorization.

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.*

There is no contractual agreement between the VA and the CSP. The agreement is between the VA and the SaaS solution vendor MARi. However, the contract between the VA and the SaaS vendor states that all data within the SaaS solution is the exclusive property of the VA and that it may not be utilized any in form without specific permission from the VA. The contract identifier is 36C19B21C0050.

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.

MARi owns ancillary data as defined by NIST SP 800-144. This data is stored and secured within the GCP FedRAMP authorized environment.

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.

The security and privacy of VA data is maintained within the SaaS application, residing on the FedRAMP authorized GCP. VA data is provided to MARi via the GCP-residing application. VA manages internal VA security and privacy risk in determining access to the MARi system. MARi manages security and risk for the MARi SaaS application, with GCP managing security and risk for the IaaS platform on which MARi is maintained.

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).

This system does not utilize 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**

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

Signature of Responsible Officials

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

Jacqueline K. Levett 3566386

Digitally signed by Jacqueline K. Levett 3566386
Date: 2023.10.24 06:57:32 -07'00'

Privacy Officer, Jacqueline Levett

LAWANDA WELLS

Digitally signed by LAWANDA WELLS
Date: 2023.10.24 11:57:25 -04'00'

Information System Security Officer, LaWanda Wells

AIMEE BARTON

Digitally signed by AIMEE BARTON
Date: 2023.10.25 16:44:34 -04'00'

Information System Owner, Aimee Barton

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).

https://www.federalregister.gov/documents/2021/11/24/2021-25637/privacy-act-of-1974-system-of-records

See: [Federal Register: July 28, 2000 (Volume 65, Number 146)]

[Notices]

[Page 46551-46555]

From the Federal Register Online via GPO Access [wais.access.gpo.gov]

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