Privacy Impact Assessment for the VA IT System called:

Ipsos Research-Enterprise

(Ipsos-e)

Veterans Affairs Central Office (VACO)

Office of Research and Development (ORD)

eMASS ID #1252

Date PIA submitted for review:

7/25/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.Drake@va.gov OITPrivacy@va.gov	202-632-8431
Information System Security Officer (ISSO)	George Quintela	george.quintela@va.gov	727-412-5872
Information System Owner	David Croall	David.Croall@va.gov	681-242-4094

Abstract

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

Ipsos Research - Enterprise (Ipsos-e) is a vendor-owned and operated SaaS application used by the VA for managing surveys, mailing, scanning, and returning survey results back to the VA. This service is to enhance recruitment processes for VA research studies by allowing veterans to complete and submit online surveys to express interest to participate in research studies which have been approved by Institutional Research Board (IRB). Ipsos-e provides support and resources needed to print and mail recruitment packets, survey materials, letters, and other materials to prospective participants. Ipsos-e also collects data and tracks the receipt of survey material. Ipsos-e is a service that gathers and analyzes important information to help VA administrators recognize emerging trends and make informed decisions. The research can be targeted to specialized groups and narrow market segments or performed on a much broader scale for across-the-board for big picture analysis.

The Ipsos Research ATO is being uplifted to a -E from a -I. This is the Enterprise PTA that will serve as the PTA for the Enterprise PR (PR-02268). The name of the system has been updated from "Ipsos VA Million Veteran Program (MVP) Print, Scan, & Mail Services" to "Ipsos Research – Enterprise" in order to align with the current effort to uplift the ATO for the system from a -I to a -E.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?
The IT system name is Ipsos Research -Enterprise.
The Program Office is Office of Research and Development Program Office.

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
This service will enhance recruitment processes for VA research studies by allowing Veterans to submit an online survey to express interest to participate in IRB-approved research, to provide consent to research participation, and to provide study data to research studies. This service will also track research participants through multiple phases of multi-step study procedures.

C. Who is the owner or control of the IT system or project?
The system is owned and operated by the providing SaaS vendor, Ipsos, and is controlled by the Office of Research and Development.

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?
The system stores information for up to one million individuals. The typical individuals are patients (Veterans and dependents) receiving healthcare at a VA facility who is

predetermined by VA research staff to meet eligibility criteria for a given study, such as age, sex, and presence or absence of medical conditions.

E. What is a general description of the information in the IT system and the purpose for collecting this information?
This system contains PII and PHI collected from veterans and dependents.

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.
Information is internally shared by with the Veterans Health Administration Corporate Data Warehouse (CDW) / Information and Computing Infrastructure (VINCI) and VHA Million Veteran's Program (MVP) – Recruitment and Enrolment (RNE) and externally shared with the D.G. Solutions.

G. Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?
No. Ipsos Research-Enterprise (Ipsos-e) operates solely from the AWS GovCloud.

3. Legal Authority and SORN

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

Title 38, United States Code, Chapter 73, Sections 7301, 7302, and 7303.

34VA10 / 86 FR 33015, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA" (6/23/2021) https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?
The SORN does not need amended or revised. The SORN does include cloud usage and storage.

4. System Changes

J. Will the completion of this PIA will result in circumstances that require changes to business processes?
The completion of this PIA is not expected to require changes to current business processes for VA or Ipsos CSP.

K. Will the completion of this PIA could potentially result in technology changes?
The completion of this PIA is not expected to result in technology changes. Both VA and Ipsos have robust technological infrastructure that can accommodate the requirements of this PIA.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Other PII/PHI data elements: Personal Study Identifiers

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

PII Mapping of Components (Servers/Database)

Ipsos Research -Enterprise consists of **two** key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Ipsos Research -Enterprise** and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Candidate_app_db	Yes	Yes	• Name • Last 4 of the SSN • Date of Birth • Personal Mailing Address • Personal Phone number(s) • Email address (optional) • Financial Information • Medications • Medical Records • Race / Ethnicity • Sex at birth / gender identification • Military History/Service Connection • Next to Kin • Personal Study Identifiers	VA requested survey completion.	FedRAMP moderate control set.
ORD_Vassy_201912026D	Yes	Yes	• Name • Last 4 of the SSN • Date of Birth • Personal Mailing Address • Personal Phone number(s) • Email address (optional) • Financial Information	VA requested survey completion.	FedRAMP moderate control set.

			• Medications • Medical Records • Race / Ethnicity • Sex at birth / gender identification • Military History/Service Connection • Next to Kin • Personal Study Identifiers		

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?
Information directly collected from the veterans and dependents using a paper or online survey method. Participating and providing information for research is voluntary and candidates can withdraw their participation at any time without consequences.

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.
Information is only collected from the individuals. No commercial aggregation is used.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
Yes. The survey data is analyzed depending on the type of the research. This analysis will be used to create reports of participation, common themes of findings and potentially scores of response items such as user satisfaction or engagement. The reports may also include user participation metrics, call metrics, and contact response metrics. Scores, reports, and analysis are produced against a survey group, not for individual records.

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?
Data is directly collected from the individuals using paper survey forms or online survey interface. Ipsos-s scan the paper survey responses and send it back to the VA via encrypted methods.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?
No OMB number available, but the business team is working towards mitigating that weakness.

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.
Mailing addressed transmitted from VA to Ipsos is checked using NCOA (National Change of Address) to ensure the accuracy of the mailing address.
Once research feedback is received in a paper form, it will be checked manually against identity of the participant to ensure that correct survey results are recorded. No other validation is conducted by the system. The individual research teams are responsible for conducting additional checks for accuracy.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

The only accuracy check performed by the commercial aggregator (NCOA) prior to collecting information is to validate the accuracy of the mailing addressed provided by the VA. Information in the NCOA is provided by the US Postal Service. Ipsos contractually obligated to check the accuracy of the mailing addresses provided by the VA.

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
Personal, health-related, and other patient/participant information is collected under relevant legal authorities associated with 1) individual projects and protocols as approved by appropriate regulatory committees (e.g. VA Central IRB) and 2) VA Operational and Research activities that further the mission of the agency as outlined in Title 38, United States Code, Chapter 73, Sections 7301, 7302, and 7303.

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: There is risk that information collected by Ipsos is in accurate, incomplete, and irrelevant.

Mitigation: Survey results are scanned to validate incomplete responses. In addition, participants are informed about research purpose so that they will provide accurate and relevant information at the time of the survey.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	Internal Use	External Use
Patient name	Used to identify the participant for the purposes of recruitment/enrollment and study processes	For mailing the survey requests to the participants (Sent to DG Solutions and verified using US Postal Service)
Last 4 of the SSN	Used to confirm identity	Not used
Date of birth	Used to confirm identity of person	Not used

Personal Mailing Address	Used to send study mailings to participants	For mailing the survey requests to the participants (Sent to DG Solutions and verified using US Postal Service).
Phone number	Used to contact participants about study procedures	Not used
Email address	Used to contact participant about study procedures	Not used
Financial information	Used to determine eligibility for special help programs	Not used
Medications	Used to measure study and care outcomes	Not used
Medical records	Used to determine study eligibility and measure study outcomes	Not used
Race/ethnicity	Used to enhance recruitment/enrollment of underrepresented study populations	Not used
Sex at birth/gender identification	Used to determine study eligibility	Not used
Military history/service connection	Used to confirm identity and eligibility for special help programs	Not used
Next of Kin	Used to gather family history	Not used
Personal Study Identifiers	Identify study participants	Not used

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?
Yes. The survey data is analyzed depending on the type of the research. This analysis will be used to create reports of participation, common themes of findings and potentially scores of response items such as user satisfaction or engagement. The reports may also include user participation metrics, call metrics, and contact response metrics. Scores, reports, and analysis are produced against a survey group, not for individual records.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the

individual? If so, explain fully under which circumstances and by whom that information will be used.
The system does not create 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 is encrypted in transit and at rest using FIPS-140-2 compliant methods and levels.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
The system collects and retain last 4 of the SSNs in an encrypted form.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
Data is encrypted in transit and at rest using FIPS-140-2 compliant methods and levels. Users must sign rules of behavior and attend mandatory training sessions. Ipsos AWS Gov Cloud (IAGC) is evaluated annually by third party auditors to establish compliance with FedRAMP Moderate controls.

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. 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:

<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?

Roles and user access are determined by contract requirements and project staffing requirements. Access is not given until the Rules of Behavior document is signed and access is approved by Ipsos Security Team. Account reviews monthly to deactivate dormant accounts. Reactivation requires supervisory and Ipsos Security Team approval.

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

Yes. Access request and approval is documented in Ipsos Access Policy document.

2.4c Does access require manager approval?

Yes. Access require manager approval as well as approval by Ipsos Security Team.

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

Yes, All access to PII is being monitored by Ipsos Security Operations Center (SOC).

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

The IAGC Technical Project Manager and the IAGC Security Officer.

Section 3. Retention of Information

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

3.1 What information is retained?

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

All information listed in section 1.1 will retain in the system for the duration of each approved research study.

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.*

Temporary. Disposed at the end of the fiscal year after completion of a research no sooner than 3 years but no later than 6 years after cutoff.

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.

Yes

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

Yes.

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

VHA Records Control Schedule 10-1. Series 8000.2
Disposition authority. DAA-0015 2015-0004, item 0002

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.
Data collected in paper form are either transferred back to the VA research team for retention and disposal or shredded on site as per contractual requirements.
Data collected electronically are either send back to the VA and immediately destructed or archived as per contractual requirements. All data destruction is followed by a certificate of destruction.

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.
This system does not conduct any research, testing or training. It only collects data, analyzed and send back to the VA for research studies.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: The system stores records containing PII and PHI related to Veterans and their dependents. Though minimal, there are risks associated with improper or premature record disposal and/or unintended retention of records within this system for longer than necessary violating research protocol, other regulatory requirement (e.g. FDA), contracted agreement, or VA policy.

Mitigation: Record retention and disposal policies are detailed within each protocol and/or contracted agreement associated with each study. Unless otherwise specified the system shall adhere to the Policies and Practices for Retention and Disposal of Records per VHA Record Control Schedule (RCS) 10-1, 8300.

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***
Veterans Health Administration CDW / VINCI	Recruitment, enrollment, and data collection for research studies.	• Name • Last 4 of the SSN • Date of Birth • Personal Mailing Address • Personal Phone number(s) • Email address (optional) • Financial Information • Medications • Medical Records • Race / Ethnicity • Sex at birth / gender identification • Military History/Service Connection • Personal Study Identifiers	Hypertext Transfer Protocol Secure (HTTPS)
Million Veteran's Program – MVP-RNE	Recruitment, enrollment, and data collection for MVP.	• Name • Last 4 of the SSN • Date of Birth • Personal Mailing Address • Personal Phone number(s) • Email address (optional) • Financial Information • Medications • Medical Records • Race / Ethnicity • Sex at birth / gender identification • Military History/Service Connection • Personal Study Identifiers	Secure File Transfer Protocol (SFTP)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: There is a privacy risk of unintended disclosure of data collected and/or analyzed to an incorrect VA personnel.

Mitigation: Ipsos has a stringent quality control process that only individual project managers are authorized to upload the data to the SFTP for client pick up

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	***List the purpose of information being shared /***	***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***	***List the method of transmission and the measures in***

shared/received with	***received / transmitted with the specified program office or IT system***		***routine use, etc. that permit external sharing (can be more than one)***	***place to secure data***
D.G Solutions	To mail the survey information to the participants.	• Patient Name • Mailing Address	MOU/ISA	Secure File Transfer Protocol (SFTP)

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: There is a risk of unintended disclosure of PII (name and address) during data transmission to the subcontractor for mailing services.

Mitigation: Data sharing between Ipsos and subcontractor is performed through SFTP and Ipsos has included all VA security requirements in their contract with the mailing subcontractor.

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.

Yes. Copy of the notice is given in Appendix-A 6.1

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

This PIA serves as public notice for the data collected for VA research purposes. Additionally, 34VA10, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA" published in the Federal Register shall apply. This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2021-06-23/pdf/2021-13141.pdf

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice. Individual notice associated with the collection and storing of data decided the project/study level. Each project/study notice includes brief information about the system, including its use in the project/study and its collection and storage of data elements, technical features, and limitations. (A sample notice is given in Appendix A 6.1)

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. The notice states that data will be shared with the vendor, identifies the risks of that sharing, and identifies the methods used to mitigate that risk.

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. Yes, participants may choose not to enroll in the research study, in which case their data will be removed from the system. No penalty or denial of service will be attached to such decline.

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.

When individuals enrolls in a research study, they are consenting to the research use of all of their study-related data and cannot specify specific uses or specific data types for those uses. The individual may choose not to enroll in the research study, in which case their data will not be stored in the system. A copy of the consent form is given in Appendix ##

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: There is risk that an individual may not understand or be aware that data will be collected, processed, and stored within the system, resulting in potentially unacknowledged use of Veteran personally identifiable information (PII) and/or protected health information (PHI).

Mitigation: Prior to enrollment in a research study, participants will be provided information about how their data will be used, collected, stored, and shared through a study-specific IRB-approved research protocol and HIPAA authorization and/or consent process. Such processes shall ensure individuals are informed and consenting to the collection, storage, and transmission of their data. Participants may opt not to enroll in a specific research study to prevent data from entering the system or may withdraw at any time and without penalty to prevent collection and use of data after terminating their participation.

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.
Per the SORN 34VA10, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA"
Director of Office of Research Protections, Policy and Education, Office of Research and Development, Telephone number (202) 443–5681 (Note: this is not a toll-free number).

*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.***
Once individuals provide responses to a survey, it is considered a snapshot in time and cannot be altered.

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 from the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?
This is a privacy act system.
34VA10, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA"
RECORD ACCESS PROCEDURE: Individuals seeking information regarding access to and contesting of records in this system related to research project submissions or participation in research projects may write, call, or visit the VA location where the records were initially generated.

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.
Research study participants will not have access to or be able to correct their research data stored in the system. In rare events, research participants may be contacted by individual study staff to amend study-related information if they realize incorrect or inaccurate information has been input into the system (e.g. survey responses, contact information).

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.
Research study participants will not have access to or be able to correct their research data stored in the system. In rare events, research participants may be contacted by individual study staff to amend study-related information if they realize incorrect or inaccurate information has been

input into the system (e.g. survey responses, contact information). Individuals are notified of these procedures in study-specific survey materials and websites.

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.
No formal redress is provided. Once individuals provide responses to a survey, it is considered a snapshot in time and cannot be altered.

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: While research participants will not have access to study data stored within the system, there is a risk that participants may provide inaccurate information (e.g. survey responses, contact information).

Mitigation: Individuals may contact study staff directly with accurate or updated information and/or update certain, very limited types of data from directly within the system (e.g. contact information).

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?
If assigned to a project requiring access, the request is first put in the form of a ticket for approval. First required approval is from IT Security, to ensure the person has read and signed Rules of Behavior and has taken all appropriate IT security awareness courses. 2nd approval is by the project owner, who will ensure that any VA required vetting is completed. Each VA project has different vetting and security levels. Finally, the Technical Project manager will approve the ticket for implementation, which includes what groups the user will be created with, to allow for role-based access.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?
Users from other agencies cannot obtain access to the system.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

- Domain Administrator - Manage User Accounts and SFTP Server
- AWS AMS Support - Perform System Scans, Audit Log Review and other technical support
- Ipsos Lead Researcher, Client PM - Client Project Management, Generate Data for Projects, Place Data on SFTP Server for the client.

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 do not have access to the system.

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.

Minimum – Annual privacy and security training plus Annual USPA Project training. Annual refresher on Rules of Behavior (All users) Additional role based training may include Admin level training, Contract specific training such a VA Privacy and Awareness training.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 03/04/2024
3. *The Authorization Status:* Authority to Operate (ATO)
4. *The Authorization Date:* 02/19/2024
5. *The Authorization Termination Date:* 02/18/2025
6. *The Risk Review Completion Date:* 02/14/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***
N/A

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)*
This system is FedRAMP Authorized and active on the FedRAMP Marketplace under FedRAMP ID FR2104636677.

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.*
VA owns all data stored in the system. Ownership is specified in the contract.

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 ancillary data is collected.

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.

Yes. VA has the ownership of all data stored in the system.

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 use 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

ID	Privacy Controls
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2024.08.16 12:05:13 -06'00'

Privacy Officer, Julie Drake

GEORGE QUINTELA Digitally signed by GEORGE QUINTELA
Date: 2024.08.16 14:26:22 -04'00'

Information System Security Officer, George Quintela

DAVID CROALL Digitally signed by DAVID CROALL
Date: 2024.08.19 08:17:10 -04'00'

Information System Owner, David Croall

APPENDIX A-6.1

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

Participant Name: _____ Date: _____ MVP ID:
Title of Research: Million Veteran Program (MVP) Principal Investigator: J. Michael Gaziano, M.D., M.P.H. Facility: VA Boston Healthcare System Enrollment Location:
VA CENTRAL IRB APPROVAL STAMP May 26 2023

INTRODUCTION
You are invited to join the Million Veteran Program (MVP), a national research program that is funded by the Department of Veterans Affairs. Before you decide to join, it is important for you to know why this research is being done and what it will involve. This includes any potential risks to you, as well as any potential benefits you may receive.
Read the information closely and discuss it with family and friends if you wish. Contact MVP staff if there is anything that is not clear or if you would like more details. Take your time to decide. If you decide to join, your signature on this consent form will show that you received all of the information contained, and that you were able to discuss any questions and concerns you had with MVP staff.

BACKGROUND AND PURPOSE
Genes are made of "DNA" that we inherit from our parents, making us who we are. For example, eye color, hair color, height, and some diseases are determined by our DNA. We are learning that lifestyle factors, such as the food we eat or what we are exposed to in our environments, can change our DNA and play a role in health and disease. But not everyone is affected the same. To find out why, we want to gather information from as many Veterans as possible to research why there are differences.
The purpose of MVP is to learn how genes, lifestyle, military experiences, and exposures affect health and wellness with the goal of improving health for Veterans and, ultimately, everyone. All Veterans are eligible to join, with the goal of enrolling over 1 million participants.
Research findings from MVP may help health care providers identify people with increased risk for specific diseases and allow for prevention or early treatment. In addition, learning how genes contribute to disease can lead to the development of new treatments.

MVP PROCEDURES
If you join MVP, you agree to:
• Provide up to 10 mL of blood (through a blood draw or a blood collection kit).
• Complete surveys about your health, lifestyle, military experiences, and environmental exposures, along with other factors that may impact your health.
• Allow access to your health records (VA and non-VA) on an ongoing basis.
• Be contacted in the future about other voluntary MVP and non-MVP research opportunities.

Investigator: J. Michael Gaziano, M.D., M.P.H. Facility: VA Boston Healthcare System Enrollment Location:

VA CENTRAL IRB APPROVAL STAMP May 26 2023

BLOOD SAMPLE AND HEALTH INFORMATION

• You will be asked to provide a blood sample through a standard blood draw from a vein in your arm.

• You may be given the option to provide your blood sample through a collection kit. The collection kit is allowed by the FDA for research because it has been determined to be non-significant risk. o If you are provided a blood sample collection kit at an MVP enrollment location, MVP staff will use the kit to collect your sample.

o If you choose to have the kit mailed to you (e.g., you enroll online and live far from an MVP location), MVP will securely disclose your name and address with the VA approved collection kit vendor. The vendor will mail you the kit and include packaging and postage to return the sample to an MVP approved laboratory. MVP may contact you if your sample is not received within a week or so after you have received the collection kit.

 You may be asked to complete a short form to capture information about the collection process.

• If the blood sample collected (either through the standard blood draw or the collection kit) is unusable for some reason, you may be asked to provide another sample.

• MVP will process your blood sample to capture information about your genes (DNA) and other substances. Testing on your sample is done for research purposes only.

• All samples will be stored in secure VA approved laboratories indefinitely.

• MVP will not report results (including genetic) to you or your doctor, and results will not be placed in your health record. If there are medical advances or changes to the program that may require MVP to share certain results with you, MVP will contact you directly.

• MVP will collect information from VA and non-VA databases, such as health and health-related records, or more general information, such as where you have lived and served.

• We may contact you for additional permission to access your non-VA health records.

• The data generated about you by the procedures described in this consent and the health information collected from your health records will be placed in the VA MVP Central Research Database.

VA CENTRAL IRB APPROVAL STAMP May 26 2023

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

There are rules to protect your private information. Federal and state laws and the federal medical Privacy Rule also protect your privacy. By signing this form, you provide your permission, called your 'authorization,' for the use and disclosure of information protected by the Privacy Rule.

The MVP team will collect information about you, as described in this consent form. Data collected from you will include the following:
• Protected health information (PHI) including name, phone number, address, email address, date of birth, SSN, dates of diagnoses, treatment, service, deployment, discharge
• Self-reported data from surveys
• Genetic and other information from your blood
• Information from your health records, such as diagnoses, hospitalizations, immunizations, treatments, laboratory test results, radiological findings, and medications, which may include HIV status, drug, alcohol or STD treatment, genetic test results or mental health treatment
• Data collected from Cooperative Studies Program (CSP) or other VA-funded studies that you are enrolled in, in cases where you've authorized the sharing of data
• Pharmacy records
• Information from death records including Social Security Death Master Files, National Death Index, and State Vital Statistic Registry

MVP may need to disclose information to others as required by VA research regulations. Others may include the Office of Research Protections, Policy, and Education, the VA Office of Research Oversight, the VA Central Institutional Review Board, and the local VA medical facility Human Research Protections Program.
If you express suicidal or homicidal intent, we will notify healthcare professionals or law enforcement officials, as appropriate, to protect you and others.
You will not have access to your MVP data, including blood sample and health information.
Joining MVP will not affect your VA health care. Treatment, payment, or enrollment/eligibility for benefits cannot be conditioned on you signing this authorization.
You can revoke this authorization at any time (see Voluntary Participation below). If you revoke this authorization, you will not be able to continue to participate in MVP. Authorized MVP staff can continue to use information about you that was collected before receipt of the revocation. MVP staff will not collect information about you after you revoke the authorization. Revocation will not affect your rights as a VHA patient to treatments or benefits outside of this research program.

VA CENTRAL IRB APPROVAL STAMP May 26 2023
This authorization for collection of information will expire at the end of the research program unless revoked prior to that time. The authorization to use your information already in the VA MVP Central Research Database will not expire.
DURATION OF THE RESEARCH
Your personal time involved with this research is only the time it takes you to donate a blood sample and complete the surveys.
POSSIBLE RISKS OR DISCOMFORTS
Any procedure has possible risks. The procedures you undergo as part of MVP may cause all, some, or none of the risks and side effects listed below. Rare, unknown, or unanticipated risks may also occur.

• The risks of providing a blood sample include pain, bleeding, bruising, and rarely, infection at the site where the needle is inserted. Fainting or light-headedness rarely occur. If you are injured as a result of the blood draw conducted by VA staff or VA contractors, VA will provide medical treatment for your research-related injury at no cost to you.
• Filling out surveys may result in distress when answering questions about health conditions, mental health, substance use, other difficult experiences, or discovering family health conditions of which you may not have been aware. You may skip any question that you are not comfortable answering and take breaks as needed.
• If you take the surveys in person, MVP staff will be available to assist you, if needed. MVP will not initiate care based on your responses to survey questions. Contact your health care providers for questions about your health. You may call the Veterans Crisis Line any time at 988 (then Press 1) or send a text to 838255.
• When MVP research results are published, they may show that certain groups (for example, racial, ethnic, or men/women) have genes that are associated with increased risk of a disease. If this happens, you or others may learn that you are at increased risk of developing a disease or condition. If you and/or your family members find this distressing, contact your health care provider directly about your concerns.
• There may be a risk that genetic information obtained as a result of participation in research could be used to discriminate with regard to a person's health insurance or job. However, as part of your participation in MVP, VA will not disclose your genetic information to health insurance companies, group health plans, or employers. In the rare event of a security breach, there are state, federal, and VA protections that prevent health insurance companies, group health plans, and most employers from discriminating against you based on your genetic information.
• There is a slight risk of a breach of security, and if information about you is unintentionally released, VA will not be able to guarantee that it will be protected. However, we will make every

effort to protect your confidentiality and to make sure that your identity does not become known.

POTENTIAL BENEFITS
You will not directly benefit from participating in MVP. Your blood sample(s) (including DNA and any other substances derived from it) combined with your health information may help researchers understand characteristics of any disease, condition, or illness. This may result in better ways to prevent, detect, and treat illnesses.
CONFIDENTIALITY
Taking part in MVP will involve collecting protected health information about you. This information will be protected in the following ways:
• All MVP information will be stored securely in the VA MVP Central Research Database.
• All samples and health information (VA and non-VA) will be coded (labeled in a way that does not directly identify you). Only select authorized MVP staff will have the ability to link the coded information to your identity.

• Researchers who are approved access to analyze samples and data will not receive your name, date of birth, contact information, or social security number.
• Your information will be combined with information from other MVP participants for scientific purposes. Any talks or papers about MVP will not identify you.
• MVP has obtained a Certificate of Confidentiality from the federal government. This helps protect your privacy by allowing MVP to refuse to release your name or other information outside of MVP, even by a court order. The Certificate of Confidentiality will not be used to prevent disclosures to local authorities of child abuse or neglect, or harm to self or others. The Certificate does not prevent you or a member of your family from releasing data about yourself or your involvement in MVP.

COSTS TO PARTICIPANTS
You will not be charged for any MVP procedures. For Veterans who are required to make co-payments for medical care and services by VA, these co-payments will continue to apply for medical care and services provided by VA that are not part of MVP.
PAYMENT
You will not be paid to participate in MVP. Your blood sample, health and other personal information will be used for research purposes only. They will not be sold.
Use of your information may lead to inventions or discoveries that could become the basis for new products or treatments. These inventions, discoveries, or products could become commercially

valuable and be patented and licensed. Commercially available products could also be developed based on information from your blood or DNA. However, VA has no plans to share with you any profits from these inventions, discoveries, or products.
MEDICAL TREATMENT AND COMPENSATION FOR INJURY
If you are injured as a result of your active participation in MVP, VA will provide medical treatment for your research-related injury at no cost to you. If you are injured as a result of your active participation in this program, please call the MVP Info Center at 1-866-441-6075. You do not give up any of your legal rights and you do not release VA from any liability by signing this form.
VOLUNTARY PARTICIPATION
Your choice about participation in MVP is voluntary. You may choose not to take part, and you will not lose any of your health benefits. If you decide to take part, you can change your mind at any time. Either way, your choice will not affect your care.
You may withdraw and revoke your authorization at any time. You may contact the MVP Info Center at 1-866-441-6075, write to AskMVP@va.gov (or Department of Veterans Affairs Million Veteran Program, PO BOX 6378, Chicago, IL 60680-9917), or visit a local MVP office.
If you withdraw:
• Your blood sample(s), including DNA or any other substances derived from it, will be destroyed so that they cannot be used in future research and no further testing performed.

However, coded samples sent out for analysis cannot be recalled and any data generated from those samples that have already been sent to researchers cannot be recalled.

• Researchers can continue to use information that has already been collected on you. No further health information will be collected after you end authorization.

PERSONS TO CONTACT

If you have questions about MVP, please contact the **MVP Info Center at 1-866-441-6075.** If you have questions about your rights as a participant, or you want to make sure this is an approved VA program, you may contact the VA Central Institutional Review Board (IRB). This is the board that is responsible for overseeing the safety of MVP participants. You may call the VA Central IRB toll-free at 1-877-254-3130 if you have questions, complaints, or concerns about the program. If you are experiencing a mental health crisis at any time, please contact the Veterans Crisis Line at 988 (then Press 1) or send a text to 838255.

Department of Veterans Affairs VA RESEARCH CONSENT FORM *Version Date:* Page **7 of 7** Participant Name: _____ Date: MVP ID: Title of Research: Million Veteran Program (MVP) Principal Investigator: J. Michael Gaziano, M.D., M.P.H. Facility: VA Boston Healthcare System Enrollment Location:

AGREEMENT TO PARTICIPATE IN THE RESEARCH PROGRAM

The purpose of the Million Veteran Program (MVP) and how your DNA and information will be used and stored has been explained to you. You have read the risks or discomforts and possible benefits of the program. You have been given the chance to ask questions and obtain answers. You voluntarily consent to donating a blood sample and your health and lifestyle information to VA for the research purposes described above. You also authorize the use of information from your health records (both VA and non-VA) which will be added to the VA MVP Central Research Database on a continuous basis so that your health status can be followed over time.

HELPFUL LINKS:

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

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

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

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

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