Privacy Impact Assessment for the VA IT System called:

GenISIS Assessing

Veterans Health Administration (VHA)

eMASS ID 815

Date PIA submitted for review:

Dec/09/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer (PO)	Michelle Christiano	michelle.christiano@va.gov	706-399-7980
Information System Security Officer (ISSO)	Tristan Carroll	tristan.carroll@va.gov	210-993-2068
Information System Owner (ISO)	Saiju Pyarajan	saiju.pyarajan@va.gov	857-364-5736

Abstract

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

GenISIS Assessing is a scientific computing system for genomic medical research. It currently provides over 230 High Performance Compute Cluster (HPC) compute nodes and approximately 10 Petabyte (PB) of storage with portions of system in VA Boston and Pittsburg facilities isolated behind a Virtual Local Area Network (VLAN). GenISIS Assessing provides isolated research enclaves where researchers can safely use cutting-edge prototype hardware and software to analyze genomic and clinical datasets. GenISIS Assessing serves as a data repository for genomic data from the VA's Million Veteran Program (MVP) and VA's National DNA Biorepository. GenISIS Assessing has outward facing Windows application and database servers configured according to VA standards. The outward facing application servers serve as gateways to isolated internal research enclaves.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

The business purpose of GenISIS is to provide a scientific computing system for genomic medical research in the Department of Veterans Affairs, specifically the Veterans Health Administration to ensure the highest regard for research volunteers' privacy.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

VHA.

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

The expected number of individuals who information is stored in GenISIS is all Veterans enrolled in the Million Veteran Program (MVP) which is currently over one million Veterans who provided signed informed consent and HIPAA authorization.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☐	VA Employees
☐	Clinical Trainees
☐	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

D. What is a general description of the information in the IT system and the purpose for collecting this information?

GenISIS is a scientific computing system for genomic medical research and is used to provide an isolated research enclaves where researchers can securely and safely use cutting-edge prototype hardware and software to analyze genomic and clinical datasets. GenISIS serves as a data repository for genomic data from the VA's Million Veteran Program (MVP) and VA's National Biorepository.

E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

Information sharing is conducted by GenISIS with the following Systems:

- VA Information and Computing Infrastructure (VINCI) via Microsoft SQL Server database connection (TDS over SSL).
- VHA (Veteran's Health Administration) (VA Corporate Data Warehouse (CDW)) via Microsoft SQL Server database connection (TDS over SSL).
- Million Veteran's Program (MVP) Patient Recruitment and Enrollment (RNE) Assessing (MVP RNE) via Microsoft SQL Server database connection (TDS over SSL).
- VA Albuquerque Pharmacy via Windows Network Shares, (TDS over SSL).
- GenISIS Cloud Burst (GCB) via LDAP Data Interchange Format (LDIF) over SSL

F. Are the modules/subsystems only applicable if information is shared?

No

G. Is the system operated in more than one site to include primary and secondary 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 has sites in Boston and Pittsburgh. Both sites' systems are managed by the same group of administrators. The same controls are used across sites, and both utilize the honest broker system.

3. Legal Authority and System of Record Notices (SORN)

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

Privacy Act Systems of Record Notice (SORN) 34VA10, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA"

H. What is the SORN?

As stated in Privacy Act Systems of Record Notice (SORN) 34VA10 "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA", Title 38, United States Code, Section 501 is the authority for maintenance and operation of this system.

I. SORN revisions/modification

None

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

No

4. System Changes

J. Will the business processes change due to the information collection and sharing?

☐ *Yes*
☒ *No*
if yes,

K. Will the technology changes impact information collection and sharing?

☐ *Yes*
☒ *No*
if yes,

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 Information 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
- ☒ Zip Code
- ☒ 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
- ☒ Genomic Data
- ☐ Gender/Sex
- ☐ Integrated Control Number (ICN)
- ☒ Adverse Event
- ☐ Military History/Service Connection
- ☒ VA System Generated IDs
- ☐ Next of Kin
- ☐ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal Identifier (EDIPI)
- ☒ Other Data Elements (list below)

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

Other PII/PHI data elements: <<Add Additional Information Collected but Not Listed Above Here (For Example, Biometrics)>>

- Administrative and billing data
- Patient demographic factors
- Prescription
- Progress notes
- Vital signs
- Medical histories
- Diagnoses
- Medications
- Immunization dates
- Radiology images
- Lab and test results

1.2 List 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?

Specimens from Participants for Bio-banking.
Electronic Medical Records/Health Information from VHA Databases
Survey Information Collected Directly from Participant
Results from Other VHA Research and Studies
Data Added to GENISIS from Other Researchers
The data is collected in accordance with the IRB approved informed consent form (ICF) or document (ICD) as well as the HIPAA Authorization. The HIPAA Authorization may be combined with the ICF/ICD or may be a separate VA Form 10-0493, Authorization for Use & Release of Individually Identifiable Health Information for VHA Research, referenced by the system administrator as a source document.

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.

Specimens from Participants for Bio-banking.
This information is received directly from the analysis of the specimens collected from the Veterans.

Electronic Medical Records/Health Information from VHA Databases
The Electronic health information needed for the MVP studies are obtained from VA sources like CDW/VINCI/VIReC. Data are not brought into GenISIS unless there is a specific need for the information.
Health information from other sources such as non-VA EHRs (electronic health record) and other available sources such as geo-spatial data are requested as required.

Results from Other VHA Research and Studies
Information from other VA research studies can be brought into GenISIS for analysis as requested by the particular study team. Research data from studies may only be added to or used in GenISIS, as detailed in the consent and/or HI PAA authorization under which the data were obtained or collected, or in accordance with the waiver of consent and/or HIPAA authorization approved by the IRB and/or Privacy Board, as applicable.

Data Added to GenISIS from Other Researchers
Finally, the fifth source of information would be research/analysis results that include data generated during the conduct of research, such as scores, computed metrics, etc., for MVP. This knowledge base will hold all aggregate published or unpublished results from all previous MVP studies and can be queried at the aggregate level thus allowing researchers to build on the previous study results.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

The GenISIS system produces curated data sets appropriate for research in the form of a data release.

1.3 Methods of information collection

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?

Specimens from Participants for Bio-banking
Specimens are collected from the individuals who volunteer to take part in the approved research projects.

Electronic Medical Records/Health Information from VHA Databases
Data from VHA data bases are transmitted over the VA network between VA systems.

Survey Information Collected Directly from Participant
Survey information is collected directly from participants through paper forms converted to electronic format. Conversion may be from scans or direct data entry. Contractors are used to collect and transmit survey results to the VA. Future plans include Web based surveys.

Results from Other VHA Research and Studies
Results from other VHA research and studies is electronically transmitted via the VA network.

Data Added to GenISIS Assessing from Other Researchers
Data added to GenISIS from other researchers is collected electronically and transmitted via the VA network.

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 physical forms are ingested by GenISIS

1.4 Information checks for accuracy, and 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.

Self-reported data, including survey data, are recorded in raw form and may be cleaned and curated for research use. As participants are enrolled, informed consent and HIPAA authorization forms are scanned by field site staff and sent to the Clinical Epidemiology Research Center (CERC), which is a MVP coordinating center, to be checked for accuracy and completeness by both electronic data checks as well as manual validation. This information is used for the governance of all use of the participants' data. All MVP data held within GenISIS Assessing is research data and both electronic and manual checks are performed at multiple steps on the data to ensure that there are no systemic errors. Scientific data quality checks are also performed on all the data and metadata about the quality of the data is provided to the researcher at the time of an approved study marts.
Data obtained from CDW/VINCI has quality checks performed at the time of creation or entry of the data at the point of care within the local VistA/CPRS system. There are no additional quality checks for accuracy of the copy of CDW/VINCI data within GenISIS Assessing.

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?
No

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

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

The authority for the system is Veterans' Benefits: Functions of Veterans Health Administration, 38 U.S. Code § 7303, which states, in part:
(a)(1) In order to carry out more effectively the primary function of the Administration and in order to contribute to the Nation's knowledge about disease and disability, the Secretary shall carry out a program of medical research in connection with the provision of medical care and treatment to veterans. Funds appropriated to carry out this section shall remain available until expended.

(2) Such program of medical research shall include biomedical research, mental illness research, prosthetic and other rehabilitative research, and health-care-services research.
The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule permits the use of protected health information for research purposes pursuant to a HIPAA authorization, which is obtained from individual patients under the MVP research study to access, collect and store their health information and blood sample(s) for future research use.

As stated in Privacy Act Systems of Record Notice (SORN) 34VA10, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA", Title 38, United States Code, Section 501 is the authority for maintenance and operation of this system.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: The VA Central Institutional Review Board (IRB) is the IRB of record and provides approval for the MVP research study in accordance with the Common Rule to ensure human subjects protections. The VA Central IRB reviews the privacy risks for the study and makes recommendations to mitigate risks to the privacy of a study participant.

During this Privacy Impact Assessment (PIA), VHA identified several potential privacy risks associated with MVP and GenISIS Assessing. The steps taken to mitigate these risks are addressed in the sections that follow. Risks include:

- The re-identification of information linked to a specific individual, notwithstanding representations that a participant's information would be anonymous or not identifiable in GenISIS Assessing as part of a particular research study.

- Use of emerging forensic methods such that a third party with access to a sample of an individual's DNA could use DNA sequence data of the type collected and shared in GenISIS Assessing to determine that the sample belongs to a specific biobank participant.
- The unpredictability of the changing risk landscape, particularly regarding the emergence of new methods enabling re-identification of de-identified study data through DNA and other factors.
- The identification of a cohort or group of participants that is small enough to narrowly define such that assumptions can be made regarding certain participants that are in that group even if individuals are not identified.

Mitigation: The Million Veteran Program is careful to only collect the information necessary to complete the mission of MVP in accordance with the IRB approved research protocol.

The VA maintains an Incident Response Plan (IRP) which is a formal document that includes the agency's policies and procedures for reporting, investigating, and managing a breach. This includes the responsibility for employees and contractors to report a suspected or confirmed breach, as well as the process and procedures that must be followed when reporting a breach. All individuals with access to Federal Information and Information Systems at VA must report a breach immediately upon discovery. Once an incident is reported, the VA makes all efforts to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA can better protect the individual's information.

GenISIS Assessing is governed by VHA Security, Privacy, and Identity Management requirements and is evaluated according to VA Handbook 6500. Mitigations include following Federal NIST security requirements including encryption, access control, isolation of data, firewalls, virtual LANS and extensive security monitoring and analysis.

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
Electronic Medical Records (EMR)	• Provides information on participant's medical history including current medical data, past history of medical issues,	Not Used

	family history, and other relevant health information. • These data are used to track how a participant's health changes over the course of time, and how those changes, when considered along with environmental and genetic factors, may help us discover better ways to detect or treat diseases. • Allows VA researchers to conduct a more robust cause-effect analysis by looking at patterns that develop while reviewing health records of the large number of participants involved in MVP	
Genomic/Molecular Data	• Provides information the genetic make-up of the participant. • The data is used by researchers to correlate biologica1/physiological outcomes to their genetic makeup. Such correlation can be used to understand and establish potential causes of diseases. • Allows researchers to design individualized treatments for more effective healthcare.	
Baseline Survey Data	• Supplements data obtained from Electronic Medical Records (EMR) • Provides a starting context for each participant in the program. This will allow researchers to better understand the changes that are occurring to an individual over time by comparing those changes relative to the starting health of the individual.	
Lifestyle Survey Data	• Optional survey that obtains information on lifestyle such as sleeping habits, alcohol consumption, smoking, etc. • Provides some additional information that is not included in	

	the baseline survey. This information would be considered useful to have by the researchers, but not absolutely necessary.	
Other Research Data	• Research results from other MVP or previous research studies are used to build future studies more efficiently and effectively. • GenISIS knowledge base will provide coded data from MVP studies that can be queried by other researchers at the aggregate level in preparation of future research to build on already conducted analysis	
Social Security Number	• Identifiable information like the Names, SSN, date of birth etc. are stored separate from other data in GenISIS. VA currently uses the SSN as the unique patient identifier or medical record number; therefore, SSN are used for ensuring the correct identification of the individual at the time of recruitment to MVP and when any data is brought into GenISIS from the primary sources like CDW/VINCI etc.	

2.2 Describe the types of tools 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?

The System analyzes genomic information and creates anonymized data sets tailored to specific research studies.

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.

GenISIS Assessing uses various electronic tools to assemble and integrate the required data into a study mart. Genomic study algorithms are created to conduct research. Within a study mart researcher use various analysis tools to conduct their research. Any research results generated during the conduct of the study will be published in peer reviewed research journals for the advancement of knowledge in the research community following all policies and procedures for conduct of human subjects' research.

Tools include statistical analysis software, custom created genetic analysis software, SQL data bases and other analytic tools for correlating medical information with genetic data to accomplish research goals. Resulting information will not be placed back into the individual's medical record nor will it affect the individual's status or benefits.

2.3 How the information in the system is secured.
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

Data in transit is protected by TLS. Data at rest is protected with full-disk encryption. The ISO and/or Designee is responsible for ensuring the systems are compliant with FIPS 140-2.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

SSNs are stored in encrypted databases behind a default deny firewall. Access is controlled via role-based access control and minimum need to know.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
GenISIS complies with federal OMB standards.PII/PHI is stored inside the Genisis secure enclave and protected using role-based access control. PII/PHI is encrypted at rest.

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?

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?

Access to the PII is determined by an individual's roles and responsibilities within the system.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Criteria, procedures, controls, and responsibilities regarding access are documented as artifacts in eMass.

2.4c Does access require manager approval?

» Authorized users of GenISIS are researchers who have completed a background screening, initial VA Privacy and Information Security Awareness and Rules of Behavior training and an authorized access request.
» In addition, all GenISIS users must be approved by the Principal Investigator (PI) who administers the research study and by the Institutional Review Board (IRB) prior to granting user access.
» System Administrators are designated for the management of information system accounts. Only System Administrators are authorized to create, enable, modify, disable and remove information system accounts upon receipt of an access request from Million Veteran Program coordinator, who is responsible for credential verification by the PI and the IRB.
» Account permissions are managed using Group Policy. GenISIS establishes conditions for each group based on study requirements and each account as identified on the request and reviewed/approved by the PI.
» Million Veteran Program (MVP) coordinators notify system administrators by email when user accounts are needed to be created, no longer required, when users are terminated or transferred and when user's information system usage or need-to-know changes.
» Authorized access to GenISIS information system is based on a valid authorization, intended system usage and other attributes, as required by VA access control procedures.
» GenISIS Standard User Accounts are managed LDAP group policies by the system administrators.
» Privileged access is requested using the MyVA Elevated Privilege request in ePAS with automated workflows in place. Notifications are sent to the Supervisor and System Owner or designee for approval using automated emails generated from the system.

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

GenISIS Assessing audit records include additional detailed information when the information is explicitly needed for specific audit requirements as indicated below:

- Full-text recording of privileged commands;
- Individual identities of group account users;
- User of root accounts instead of Non-Mail Enabled Accounts (NMEA);
- Local administrator account still uses administrator as account name;

• Security enabled local group member added.
» User Activity log – Reviewed by a GenISIS Assessing Administrator in collaboration with the ISSO on a quarterly basis. If there are any discrepancies, the GenISIS Assessing Administrator will investigate further and provide a report that reflects potential violations to the ORD ISSO.
» The report from GenISIS Assessing includes session, username and ID, template accessed, request arguments, referrer, client browser, remote address, and date time stamp.
» Suspicious activities may include, but will not be limited to identification of:
• Multiple failed login attempts
• Multiple passwords reset requests
• Suspicious website requests
» Change control records – Version control change/update records, RFCO requests, and integrity verification records between repository and production. Included in the Validation Protocol for each Research project application are records that address non-repudiation; information system design documentation; information system configuration settings and associated documentation; validation records; information system audit records; and other relevant documents or records. If there are any discrepancies, the GenISIS Assessing Administrator will investigate further and provide a report that reflects potential violations, if any to the ORD ISSO.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

Information System Owner (ISO)
» Monitors and investigates security violations for activities involving access and modification of files within the information systems.
» Determine and enable audit logs at the GenISIS Assessing system level, and document what audit events will be monitored for Network applications.
» Determine and implement audit logs events.
» Determine privilege users with authorized access to management of audit functionality at GenISIS Assessing system level.

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 collected from question 1.1 is retained by the system.

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

GenISIS scientific servers that are managed by GenISIS system administrators retain information up to 6 years in accordance with the Records Control Schedule 10-1 or to a duration specified by the research project or contractual requirements.

3.3 The retention schedule 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. Please work with the system 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?

Yes
https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf.

3.3b Please indicate each records retention schedule, series, and disposition authority?
34VA10, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA" published in the Federal Register. This SORN can be found online at https://www.gpo.gov/fdsys/pkg/FR-2010-05-27/pdf/2010- 12758.pdf

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated, or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Records are destroyed according to NIST 800-88 standards including hard drive degaussing and shredding and VA Directive 6371 regarding destruction of temporary paper records. Destruction of hard drives and paper are accompanied by 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 is evaluated according to NIST 800-53 and VA Directive 6500 for security. Records are destroyed according to RCSIO-1 schedules. GENISIS is a restricted access data and computational system. Any data contained within GENISIS is partitioned to allow for role-based access. Each research study is approved by the Institutional Review Board (IRB) before analysis is conducted.

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 Privacy Officer (PO) 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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe 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 privacy risk is that sensitive data will be kept longer than necessary and thus would be subject to risk for a longer time period.

Mitigation:
Mitigations include following Federal NIST security requirements including encryption, access control, isolation of data, firewalls, virtual LANS and extensive security monitoring and analysis. This information is carefully managed to only store the information necessary to complete the studies in accordance with IRB approved protocols. Information listed in section 1.1 is retained according to the Records Control Schedule (RCS 10-1) and then destroyed according to NIST 800-88 standards and VA Directive 6371 regarding destruction of temporary paper records. Destruction of hard drives and paper are accompanied by a certificate of destruction. GenISIS maintains an incident response plan for reporting, investigating, and managing a breach.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a GenISIS consists of 3 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 GenISIS 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 3.9a 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
GenISIS SQL databases	Yes	Yes	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Fax Number • Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Current Medications • Previous Medical • Records	To support Million Veteran Program (MVP), a volunteer-based and VA sponsored national research program for Genomic studies.	Secure information according to NIST 800-122/FISMA standards Data access points are within VA VLANS ad behind VA firewalls. SQL databases encryption. Access control per role/group permission approved by VA central institutional

			• Race/Ethnicity		Review Board (IRB).
Genomic HPC analytics environment	Yes (data records collected in this environment are deidentified)	Yes	• Demographic factors • Progress notes • Medical Records and History • Diagnoses • Current Medications • Radiology images • Race/Ethnicity • Lab and Test Results • Genomic Data	To support Million Veteran Program (MVP), a volunteer-based and VA sponsored national research program for Genomic studies.	Secure information according to NIST 800-122/FISMA standards Data access points are within VA VLANS ad behind VA firewalls. SQL databases encryption. Access control per role/group permission approved by VA central institutional Review Board (IRB).
Honest Broker	Yes	Yes	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Fax Number • Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Current Medications • Medical Records	To support Million Veteran Program (MVP), a volunteer-based and VA sponsored national research program for Genomic studies.	Secure information according to NIST 800-122/FISMA standards Data access points are within VA VLANS ad behind VA firewalls. SQL databases encryption. Access control per role/group permission approved by VA central

			• Race/Ethnicity • VA system generated IDs		institutional Review Board (IRB).

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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***
VA Information and Computing Infrastructure (VINCI)		• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Fax Number • Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Current Medications • Previous Medical Records	Microsoft SQL Server database connection (TDS over SSL).

		• Race/Ethnicity • Vital signs • Diagnosis • Immunization dates • Lab and Test Results	
VHA (Veteran's Health Administration) (VA Corporate Data Warehouse (CDW))		• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Fax Number • Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Current Medications • Previous Medical Records • Race/Ethnicity • Vital signs • Diagnosis • Immunization dates • Lab and Test Results	Microsoft SQL Server database connection (TDS over SSL).
Million Veteran's Program (MVP) Patient Recruitment and Enrollment (RNE) Assessing (MVP RNE)		• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Fax Number • Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Current Medications • Previous Medical Records • Race/Ethnicity • Prescription • Adverse Event	Microsoft SQL Server database connection (TDS over SSL).
VA Albuquerque Pharmacy		• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Fax Number • Email Address • Emergency Contact Information (Name, Phone	Windows Network Shares, (TDS over SSL).

		Number, etc. of a different individual) • Current Medications • Previous Medical Records • Race/Ethnicity • Prescription • Adverse Event	
GenISIS Cloud Burst (GCB)		User Metadata: • Name • Mailing Address • Zip Code • Phone Number(s) • Fax Number • Email Address	LDAP Data Interchange Format (LDIF) over SSL
VA Cooperative Studies Program (CSP)		• Name • Social Security Number • Date of Birth• Mailing Address • Zip Code • Phone Number(s) • Fax Number • Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Current Medications • Previous Medical • Records• Race/Ethnicity • Prescription • Adverse Event	Windows Network Shares, Microsoft SQL Server database connection (TDS over SSL

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk:

Retrieval of information from other VA sources results in some data being stored in two locations. Also, movement of data across networks creates additional opportunities for data loss or breach.

Mitigation:

Records are destroyed according to RCS-10 schedules to reduce the amount of time data exists in two locations. When no longer needed, records are destroyed according to NIST 800-88 and VA directive 6500 and other VA standards. VA data is transmitted via VA internal secure networks.

These networks are operated and maintained according to NIST 800-53 and VA Directive 6500. Incidents are reported and managed according to an official Incident Response plan. Additionally, VA network traffic is monitored by security teams on a 24-hour basis.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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***	***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***	***List the method of transmission and the measures in place to secure data***

	office or IT system		***be more than one)***	
Knowledge Discovery Infrastructure (KDI) Department of Energy (DOE)		• Name • Social Security Number • Date of Birth • Race/Ethnicity • Vital Signs • Diagnosis • Current Medications • Immunization Dates • Lab and Test Results • Contact Information (Mailing Address, Zip Code, Email Address, Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Genetic Information	MOU/ISA/IAA	Point-to-Point VPN
IPSOS Research - Enterprise		• Name • Mailing Address • Contact Information (is shared with IPSOS and IPSOS manages surveys and returns data to VA) • Survey data	Encrypted communication over email.	MOU **AOU group has an agreement with IPSOS.**

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 impermissible disclosure, i.e., legal authority is not present, associated with sharing information outside of VA.

Mitigation:
Mitigations include following Federal NIST security requirements including encryption, access control, isolation of data, firewalls, virtual LANS and extensive security monitoring and analysis. External connections are protected with encrypted VPN tunnels and controlled by Memorandums of Understandings and Interconnection Security Agreements (MOU/ISA) to assure proper protection of data throughout the data transfer. Some data is shared via FIPS 140-2 encrypted hard drives and other approved encryption methods.
An approved IRB protocol has been received outlining the data to be obtained along with Privacy Officer (PO) review for a determination that legal authority exists prior to disclosure.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

Privacy Notice is handled by MVP RNE.

MVP is a completely voluntary program, and as such extensive efforts are made to provide potential participants in MVP with detailed notice about the program and the data collection and use practices associated with MVP. Notice is provided through: (1) invitation letters sent to potential participants; (2) a brochure explaining the nature of the study; (3) consent form(s); (4) Privacy Act Statement of Records Notice(s); (5) Privacy Act Statements on forms as appropriate; (6) face-to-face conversations; (7) information generally available on VHA's website; and (8) this Privacy Impact Assessment.
MVP sends potential participants an invitation letter to take part in the program. Participants must execute a consent form before participating. On the day of the study visit, during the informed consent process, member(s) of the research staff who have been trained and approved to obtain participant consent discuss the purpose, methods, risks, and future benefits of MVP with the Veteran. At specified recruitment sites Veterans are currently being encouraged to "walk-in" and learn about the program. This strategy includes active approaches, such as having study personnel discuss MVP face-to-face with Veterans and VA clinicians. Potential participants are given adequate time to review and discuss the informed consent document and the study at the time of the (impromptu) study visit.

The VA Privacy Service Office conducts outreach campaigns geared towards Veterans and VA employees, increasing and developing more effective communications tools for targeted audiences to raise privacy awareness and strengthen VA's standing as a trusted government agency. Through their public website, Privacy Services provides a touch point for Veterans with regard to privacy practices. VA provides public notice regarding MVP and GENISIS through: The template for VA Form 10-1086 can be found at: http://vaww.va.gov/vaforms/medical/pdf/vha-10-1086.pdf.2. VA has published in the Federal

Register the Privacy Act Systems of Records Notice (SORN) SORN 34VA10, Veteran, Patient, Employee, and Volunteer Research and Development Project RecordsVA. This SORN can be found online at https://www.gpo.gov/fdsys/pkg/FR-2010-05-27/pdf/2010- 12758.pdf.3. This Privacy Impact Assessment (PIA) also serves as notice of the RNE application. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."4. VHA Notice of Privacy Practice is given to all enrolled Veterans every three years, upon request or when there is a significant change to the Notice. A copy of the Notice of Privacy Practices is available online at http://www.va.gov/health

6.1b If notice was not provided, explain why.

Notice is provided

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

Notice provided informs individuals that their information will be used for research. Genisis is a research platform.

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.

All enrollment is handled by MVP RNE

MVP participants must sign an Informed Consent on VA Form 10-1086 to participant in the research study, and to have their information placed in GENISIS as participation is completely voluntary. In addition, MVP participants must also complete a VA Form 10-0493, Authorization for Use and Research of Individually Identifiable Information Collected for VHA Research, in order for MVP to collect and use the participants' health information in GENISIS. Signature on the authorization is completely voluntary and can be revoked at any time.

Page 7 of VA Form 10-1086 (informed consent form), indicates participants can leave the program at any time. At the time of consent, participants also receive a copy of the form, "MVP Withdrawal Form (Revocation of Authorization For Release of Protected Health Information For

Research Purposes and Sample Withdrawal)" and are instructed to complete and return that form (or contact the MVP Information Center) if they wish to withdraw from MVP.

VA Form 10-0493 indicates participants can revoke their authorization at any time by submitting a revocation request in writing. VA Form 10-10116, Revocation of Authorization for Use and Release of Individually Identifiable Health Information for VHA Research

Both data collection and data use will cease once an MVP participant withdraws from the study and revokes HIP AA authorization. However, data that has already been used in an MVP research study will be maintained in GENISIS for the research record retention period. Opting into the program is a yes-or-no proposition, and there are no tiers for selective participation in this project.

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.

Consent is collected by MVP RNE. Each subject provides written informed consent for the research activity, or the IRB approves a waiver of informed consent in compliance with federal regulations.

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 Privacy Officer (PO) 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: This is referring to sufficient notice provided to the individual.

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

Privacy Risk:
There is a risk that members of the general public may not know that GenISIS exists within VA despite publication of information in a public forum. Additionally, there is a risk that Veterans were not given adequate notice their information was collected for use.

Mitigation:
>> MVP participants must sign an IRB approved Informed Consent Form to participant in the research study, and to have their information placed in GenISIS as participation is completely

voluntary. In addition, MVP participants must also complete a VA Form 10-0493, Authorization for Use and Research of Individually Identifiable Information Collected for VHA Research, for MVP to collect and use the participants' protected health information (PHI) in GenISIS. Signature on the authorization form is completely voluntary. The VA also mitigates this risk of not providing adequate notice to the public in two ways, as discussed in detail in question 6.1 above; specifically, the PIA and SORN are published to notify and inform the public that information collected by the VA.
Active participants in approved research studies are given notice and informed consent forms prior to their information being collected for the approved research study.
Notice of collection for research studies is recorded on the informed consent form.
The VA Privacy Service Office conducts outreach campaigns geared towards Veterans and VA employees, increasing, and developing more effective communications tools for targeted audiences to raise privacy awareness and strengthen VA's standing as a trusted government agency. Through their public website, Privacy Services provides a touch point for Veterans regarding privacy practices. Veterans may use this portal to research all VA Systems of Records (SORN) by accessing the Privacy Services page (VHA SYSTEM OF RECORDS (sharepoint.com)).

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***
We follow VA FOIA practices. GenISIS does not have any additional access provisions.

Requests for copies of VHA records, including research records, must be in writing from the individual to whom the records pertain. All requests must be referred by the System Manager for the concerned VHA Privacy Act system of records, the facility Privacy Officer, or their designee to the appropriate employee who determines whether the right of access request will be granted. Individuals will either receive the copy of records or an acknowledgement letter indicating when the records will be provided within 10 working days. Ref. VHA Handbook 1605.1 Para. 7.
MVP Participants wishing to access their MVP information may write or call the Director of Operations, Research and Development (12), Department of Veterans Affairs, 810 Vermont Ave., NW Washington, DC 20420 as directed in the Privacy Act SORN 34VA10 "Veteran, Patient, Employee,

and Volunteer Research and Development Project Records-VA." This SORN can be found online at https://www.gpo.gov/fdsys/pkg/FR-2010-05-27/pdf/2010- 12758.pdf.3.
The procedure outlined in the Privacy Act SORN 34VA10 complies with VHA Handbook 1605.01 Para. 7 and VA Regulations at 38 CFR § 1.577.
In addition, MVP Participants may contact the Information Center toll-free number, or the MVP Principle Investigators or Local Site Investigator to request copies of their MVP research records. This information is provided to the MVP Participant during the Informed Consent process.

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)?

GenISIS 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?

GenISIS 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.
MVP Participants are made aware of procedures for correcting their information in multiple ways. First, this information in published in the Privacy Act SORN 34VA10, "Veteran, Patient, Employee and Volunteer research and Development Project Records -VA" in the Federal Register. In addition, all Veterans are provided a VHA Notice of Privacy Practices (NOPP) every three years, upon request or when significant changes are made. The VHA NOPP provides information on how to request and amend to their health information maintained by VHA. Lastly, this information is contained in VHA Handbook 1605.01, Privacy and Release of Information, which is available to the public online at http://www.va.gov/vhapublications/publications.cfm?pub=2&order=asc&orderby=pub _

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.

Individuals are made aware of procedures for correcting their information in multiple ways. First, this information in published in the Privacy Act SORN 34VA10 Veteran, Patient, Employee and Volunteer research and Development Project Records -VA" in the Federal Register. In addition, all Veterans are provided a VHA Notice of Privacy Practices every three years, upon request or when significant changes are made. The VHA NOPP provides information on how to request and amend to their PHI maintained by VHA. Lastly, this information is contained in VHA Handbook 1605.01, Privacy and Release of Information, which is available to the public online at

http://www.va.gov/vhapublications/publications.cfm?pub=2&order=asc&orderby=pub_

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.

Formal redress is provided as stated above in section 7.3

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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk:
The individual may also seek to access (or redress) records about them held within the GENISIS and become frustrated with the results of their attempt.

Mitigation:
Active participants in VA research studies can redress and correct information directly with the study's research staff. Through informed consent and HIPAA authorization forms, the active participants are informed of what information is being collected for the study and what purpose the information will be used for.
Strict policy defined in VHA 1200.05, Requirements for the Protection of Human Subjects in Research, mitigates the risk that information collected for a study will be used for other purposes.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

Upon IRB approval, GENISIS users will be provisioned with account and access based on their approved roles:
System Administrator: user provisioning/de-provisioning, software installs, system upgrades, security patches, HPC systems design, implementation and maintenance.

- Research Study Group Member: membership per study is approved by VA ORD IRB. This role has access to GENISIS Analytic environment - workspace and datasets are provisioned only accessible for the study which the user is a member of.
- Data Stewards: each study group has elected data stewards who has additional responsibility and privilege to review and transfer research summary finding to network shares. No PH/PHI data outbound from Genisis is allowed.
- Data Operations: any operations that are data related, such as manage raw data intake, catalog genomic data, extract, transform and load (ETL) to and from data sources.
- Honest Broker Operators: Before data sets delivered to study marts, Honest Broker Operators run through honest broker processes to crosswalk identifiers to be study mart specific identifier. This is to prevent/reduce the chance for data triangulation.
- DevOps: Genisis development and operations consist of HPC experts, bioinformaticians, system engineers, software engineers and Data/Bio-Computational scientists to support and maintain day-to-day operations as well as longer terms Genisis development needs.

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 do not have access to the system.*8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.*
The following information system accounts are used to support the GENISIS' Mission/business functions:
• Standard User Accounts (SUA) – issued for routine non-privileged access. These accounts are enforced password authentication.
• Administrator Accounts – issued to accomplish administrative tasks requiring privileged access to GenISIS
• Service Accounts – used by a service, program, application, or other process requiring authentication. Service accounts must have an identified Account Custodian.

• Honest Broker Account-Privilege accounts that has access to sensitive data.

» Authorized users of GenISIS are researchers who have completed a background screening, initial VA Privacy and Information Security Awareness and Rules of Behavior training and an authorized access request.
» In addition, all GenISIS users need to be approved by the Principal Investigator (PI) who administer research study and by the Institutional Review Board (IRB) prior to granting user access.
» System Administrators are designated for the management of information system accounts. Only System Administrators are authorized to create, enable, modify, disable, and remove information system accounts upon receipt of an access request from Million Veteran Program coordinator, who is responsible for credential verification by the PI and the IRB.
» Account permissions are managed using Group Policy. GenISIS establishes conditions for each group based on study requirements and each account as identified on the request and reviewed/approved by the PI.
» Million Veteran Program coordinator notify system administrator by email when user accounts are needed to be created, no longer required, when users are terminated or transferred and when user's information system usage or need-to-know changes.
» Authorized access to GenISIS information system is based on a valid authorization, intended system usage and other attributes, as required by VA access control procedures.
» The following reviews are performed on account reports from the System Administrator by the ISSO:
• New User Access Requests (monthly)
• Privileged Account Reviews (quarterly)
• Separated User Reviews (quarterly)
• Inactivity Account Reviews - >90 and 180 days (monthly)

8.2a. Will VA contractors have access to the system and the PII?

VA Contractor access is verified through VA personnel before access is granted to any VA contractor. Contracts and contractor access are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access

8.2b. What involvement will contractors have with the design and maintenance of the system?

VA Contractor access is verified through VA Human Resources before access is granted to any VA contractor. Contracts and contractor access are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. In Addition, contractors are required to complete a GenISIS specific Rules of Behavior. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

8.2c. Does the contractor have a signed confidentiality agreement?

Yes

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

No

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
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.

No

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 requires researchers to undergo annual mandatory trainings in research ethics, privacy and HIPAA, and security. These trainings are provided via the online CITI program as well as the VA's Talent Management System (TMS). VA workforce members, including contractors, will be required to take the VA Privacy and Information Security Awareness Training and Rules of Behavior (VA l0l76), which covers general privacy requirements and security within VA, and the Privacy and HIPAA Focused Training (VA10203), which is a more intensive privacy training that addresses HIPAA requirements. If needed, researchers may also meet with the VA's National Center for Ethics in Health Care.
In order to access the system, researchers must also undergo "GenISIS User Training" provided by GenISIS staff. They must also adhere to the GenISIS rules of conduct.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status: Approved*
2. *The System Security Plan Status Date:* May/17/2024
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date: October/8/2024*
5. *The Authorization Termination Date:* October/08/2025
6. *The Risk Review Completion Date:* June/07/2024
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.***

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. ***(Refer to question 1.8 of the PTA)***

No

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Not applicable as the system does not use cloud technology.

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.

Not applicable as the system does not use cloud technology.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Not applicable as the system does not use cloud technology.

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).

Not applicable as the 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
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.

MICHELLE CHRISTIANO

Digitally signed by MICHELLE CHRISTIANO
Date: 2025.01.13 07:19:16 -05'00'

Privacy Officer, Michelle Christiano

TRISTAN CARROLL

Digitally signed by TRISTAN CARROLL
Date: 2025.01.13 10:20:40 -06'00'

Information System Security Officer, Tristan Carroll

SAIJU PYARAJAN

Digitally signed by SAIJU PYARAJAN
Date: 2025.01.13 08:23:15 -05'00'

Information System Owner, Saiju Pyarajan

APPENDIX A-6.1

Register the Privacy Act Systems of Records Notice (SORN) SORN 34VA10, Veteran, Patient, Employee, and Volunteer Research and Development Project RecordsVA. This SORN can be found online at https://www.gpo.gov/fdsys/pkg/FR-2010-05-27/pdf/2010- 12758.pdf.3. This Privacy Impact Assessment (PIA) also serves as notice of the RNE application. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."4. VHA Notice of Privacy Practice is given to all enrolled Veterans every three years, upon request or when there is a significant change to the Notice. A copy of the Notice of Privacy Practices is available online at http://www.va.gov/health

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)