



Privacy Impact Assessment for the VA IT System called:

VHA Geographic Information System (GIS)

Date PIA submitted for review:

10/12/2021

System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Andrea Mayo	andrea.mayo@va.gov	304-263-0811
Information System Owner	Nancy Leathers	352.381.5782	352.381.5782

Abstract

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

The GIS system provides tools to Veterans Integrated Service Network (VISN), strategic, and facility planners that allow them to visualize how facility location decisions spatially relate to the residential locations of Veteran beneficiaries.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *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 IT system name is VHA Geographic Information System (GIS) and the name of the program office that owns the VHA-GIS is the Geospatial Service Support Center (GSSC).
- The VHA-GIS application provides tools for strategic planners for evaluating the impact to Veterans when a VHA Healthcare site is added or decommissioned. The application can select the optimal location for a new facility given the locations of VHA enrollees’ residences and existing facilities.
- The application database stores the residential address of approximately 9.5 million enrollees but users of the application cannot see/access that data; the data are used only for analysis/processing. Only aggregated data are made available to end users.

- The system is not a regional GSS, VistA, or LAN.
- The application stores and displays VA and non-VA healthcare delivery sites, VHA geographies (VISNs, Markets, Submarkets, & Sectors), Counties, Congressional Districts, Native American Tribal lands, VHA Enrollee and Veteran populations and 10-year projected populations summarized at the county level, VHA enrollee density, and travel time bands around VHA healthcare delivery sites.
- The application does not share any information with other applications/systems.
- The VHA-GIS is a web application that is available upon request to all VHA VISN and facility planners as well as VA Central Office Strategic Planning staff.
- The VHA-GIS was granted a 1-year Authority to Operate on September 9, 2021; findings are being remediated and/or remediation plans are being documented and updated. Title 38 USC Section 501 also gives authority to collect information.
- We do not anticipate any changes to the business process because of the PIA.
- We do not anticipate any technology changes resulting from the PIA.
- There is no existing SORN.
- The application will be hosted in the Amazon Web Services (AWS) Cloud. AWS GovCloud High has been FedRAMP JAB Authorized at the High Impact Level.
- Systems/applications retain ownership of their data.
- The VA Enterprise Cloud Office manages contracts with Microsoft Azure Government and AWS GovCloud High in accordance with NIST standards/guidance.
- The magnitude of harm if privacy related data is disclosed, intentionally or unintentionally is low.

Section 1. Characterization of the Information

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

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

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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 Account Information
- Health Insurance Beneficiary Numbers
- Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications

- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Other Unique Identifying Information (list below)

Residential Address and Zip Code if different from Mailing Address.

PII Mapping of Components

VHA Geographic Information System (GIS) consists of 1 key component. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **VHA Geographic Information System (GIS)** and the functions that collect it are mapped below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Web Portal Mapping	No, it does not collect PII	Yes, it stores PII	Mailing Address and Zip Code	To conduct spatial analysis.	Portal users can see aggregated data only; individual records are used for processing only

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The Health Eligibility Center (HEC) pulls the Veteran data from the Administrative Data Repository (ADR), VA-150VA19, delivers it to the Health Systems Data and Analysis (HSDA) group (within the VHA Chief Strategy Office). HSDA processes and copies to one of the Geospatial Service Support Center (GSSC) Windows servers, which are located within the Region 03 PTA/PIA, where geospatial data are added. Enrollee data will be updated annually. Information stored in the AWS database includes the Veteran enrollee's residential address, Zip Code, latitude of residence, and longitude of residence, along with other non-PII data. Individual enrollee records are not displayed by the system, only aggregated data are displayed. Data are used only for processing.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The VHA Geographic Information System plays no part in the collection of enrollee data. Data are extracted from secure on-premise databases and transferred to the Geospatial Service Support Center (GSSC) for processing; post-processed data are transferred to the AWS database for use by the application.

1.4 How will the information be checked for accuracy? How often will it be checked?

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.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The VHA Geographic Information System uses the enrollee's geocoded residential address information along with 30 and 60-minute drive time bands to determine the number of Veteran enrollees who will be impacted by a change in the location of a healthcare delivery site. The VHA-GIS processes the information and delivers a summary report to the user. Users do not see specific information about the enrollees who will be impacted by changes in delivery sites; they have access to summary data only.

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

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

This question is related to privacy control AP-1, Authority to Collect

The VHA Geographic Information System does not collect data; it uses data collected by other systems/applications, under the authority of Title 38 USC Section 501.

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.

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The VHA Geographic Information System does not collect data from users; however, it stores personal information (residential address, zip code, and geographic coordinates) that was extracted from the Administrative Data Repository, and it uses the information to identify gaps in primary care and to determine the impact of healthcare delivery site change

Mitigation: The system will reside in a secure environment that meets all VA security standards. Users cannot access the system without a PIV card or other multi-factor authentication method. In addition, users cannot view individual enrollee records; they see only post-processed summary data.

Section 2. Uses of the Information

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

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

Identify and list each use (both internal and external to VA) of the information collected or maintained.

This question is related to privacy control AP-2, Purpose Specification.

The GIS uses the residential address information of Veteran enrollees, the location of healthcare facilities (existing and planned), and geospatial tools to find the closest healthcare facility to each Veteran enrollee. The results are summarized by facility (number of enrollees who live closer to that facility than any other), allowing planners to see which facilities in their market are ideally located and which ones should be relocated.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The system does not create or alter individual records, nor does it make new or previously unutilized information about an individual available to the end user. Instead, the system uses the location data for Veteran enrollees within a user selected area of interest and a location-allocation algorithm to determine the optimal location of healthcare facilities. The system also provides tools for assessing the impact of opening or closing a healthcare site on access to care and it allows users to create maps that display Veteran enrollee summary data, healthcare facility location, and other publicly available non-PII/PHI data.

2.3 How is the information in the system secured?

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

The VHA Geographic Information System has addressed the need for data to be stored in transit by encrypting the data. We address the need for storage at rest by encrypting the storage volumes used by the database using AWS KMS encryption keys. As such, the database is encrypted at the volume level.

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

The VHA GIS does not collect, process, or retain Social Security Numbers.

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Add answer here:

Access to databases that contain PII requires approval by system administrators as well as the data analyst's supervisor. Access is granted on a need-to-know basis and is restricted to the least amount of information required to meet the need of an intended purpose. The analyst who pulls Veteran enrollee data for the VHA Geographic Information System has had high level clearance with regards to veteran information for over 10 years. Each and every dataset must remain on either VHA or CDW servers. Violation of the security rules/procedures can result in loss of privileged access.

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

Mailing Address & Zip Code data are stored in 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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

This question is related to privacy control DM-2, Data Retention and Disposal.

The VHA Geographic Information System (GIS) relies on current data for analysis and retains only the information necessary for running analyses. Data files are updated annually so the analyses are current and relevant. The application does not store previous years' data. Previous years' data are deleted from the VHA-GIS database because they no longer have business use in accordance with RCS 10-1.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.

This question is related to privacy control DM-2, Data Retention and Disposal.

VHA-GIS follows RCS 10-1. The application does not allow access to or retrieval of individual records. Only aggregated/summary data are accessible via the application. Data used by the application are for business purposes only. When updated data are available, the prior year's data are deleted in accordance with GRS 5.2c item 020, DAA-GRS-2017-0003-0002 (<https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf>) and new data are copied to the database.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

The application uses digital data. When annual updates are copied to the database, old records are deleted from the database in accordance with GRS 5.2 item 020, DAA-GRS-2017-0003-0002; the old information is no longer needed for business use. Disposition is in accordance with GRS instruction for handling intermediary records (<https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf>)

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research? This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

The Geospatial Service Support Center uses dummy data for testing and training as an extra precaution but users don't have access to the individual records in either system – staging or production.

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.

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: There is a risk that the files containing PII will not be updated and older data will be retained longer than necessary.

Mitigation: VHA-GIS follows RCS 10-1. Previous years' data are deleted from the AWS database annually and replaced with data for the current year. The application retains analyses (impact reports) until they no longer have business value, at which time they are deleted by the end user or a system administrator. Impact reports contain no PII, only aggregated/summary data.

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 3.10 (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are shared/received with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
IT System information is received from the Administrative Data Repository (ADR)	The application stores and uses the information to identify gaps in primary care and to determine the impact of healthcare delivery site changes	PII and non-PII data; PII includes residential address, zip code, and geographic coordinates	Electronic transfer

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.

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

Follow the format below:

Privacy Risk: There is always a risk that an employee may not secure the data.

Mitigation: All users are required to take privacy and security training and sign the Rules of behavior to ensure that the data is kept safe and secure.

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 3.11 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

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are shared/received with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
None				

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: Neither application nor data are shared externally

Mitigation: None required.

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is 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.

The VHA Geographic Information System does not collect data. It gets data from the Administrative Data Repository (ADR), VA-150VA19, processes it, and uses it for analysis. However, The Notice of Privacy Practice (NOPP) is provided to all enrolled Veterans. The NOPP explains in detail the Veterans rights and how their information is collected, used, maintained, and shared. The NOPP is given out when the Veteran enrolls and when updates are made to the NOPP copies are mailed to all VHA beneficiaries.

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

The Veterans' Health Administration (VHA) requests only the minimum necessary information to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information to the VHA, this will prevent them from obtaining the benefits necessary to them. There is no penalty assessed if the Veteran chooses to withhold information however this may cause delays in care or benefits.

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

VHA permits individuals to agree to the collection of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by VHA Central Office periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations where required. Where legally required VHA obtains a signed, specific written authorization for each intended purpose from individuals prior to releasing, disclosing or sharing PII and PHI. Individuals seeking information regarding access to and contesting of VA medical records may write, call, or visit the last VA facility where medical care was provided.

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.

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 a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits and that the NOPP is mailed out when there is a major change. The VA also

mitigates this risk by providing the Privacy Impact Analysis. Individuals seeking information regarding access to and contesting of VA medical records may write, call, or visit the last VA facility where medical care was provided.

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?

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.

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).

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 question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

The VHA Notice of Privacy Practices informs Veterans of their right to obtain copies of their PII maintained in VHA records. Each VHA Privacy Act system of records notice (SORN) informs individuals how to obtain access to records maintained on them in the SORN. VHA permits individuals to obtain access to or get copies of their PII, and this is outlined in VHA policy such as VHA Directive 1605.01 Privacy and Release of Information. Individuals must provide a written request for copies of their records to the VHA facility Privacy Officer for medical records or the System Manager for the Privacy Act system of records as outlines in the notices. The request will be processed by VHA within 20 work days. The Department of Veterans' Affairs has also created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at: <https://www.myhealth.va.gov/index.html> Veterans and other individuals may also request copies of their medical records and other records containing personal data from a medical facility's Release of Information (ROI) office. Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative to obtain information upon request.

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.

VHA has a documented process for individuals to request inaccurate PII be corrected or amended and a process for review to determine if correction or amendment is appropriate. The policy complies with both the Privacy Act, VA regulations and the HIPAA Privacy Rule and is described in detail in VA Directive 1605.01 Privacy and Release of Information. Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SORN. Every VHA Privacy Act SORN contact information on Contesting Record Procedure which informs the individual who to contact for redress. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA

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.

Veterans are informed of the amendment process by many resources to include the Notice of Privacy

Practice (NOPP) which states:

Right to Request Amendment of Health Information.

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a “Statement of Disagreement”
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Information can also be obtained by contacting the facility ROI office.

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.

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

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

Veterans and other individuals are encouraged to use the formal redress procedures discussed above to request edits to their personal medical records and other personal records retained about them

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.

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

Principle of Individual Participation: *Is the individual provided with the ability to find out whether a project maintains a record relating to him?*

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

Principle of Individual Participation: *Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?*

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that a Veteran may not know how to obtain access to their records or how to request corrections to their records

Mitigation: The Notice of Privacy Practice (NOPP), which every patient receives when they enroll for care discusses the process for requesting an amendment to one's records.

VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their health records and other records containing personal information. The Veterans' Health Administration (VHA) established MyHealthVet (MHV) program to provide Veterans remote access to their health records. The Veteran must enroll in MHV to obtain access to all the available features. In addition, Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

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?

Describe the process by which an individual receives access to the system.

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

The VHA GIS application was developed for a small group of users (<1000). Most are strategic planners. To gain access to the application, the user or the user's supervisor requests access from a system administrator. The application is behind the VA firewall and is accessible only to VA staff. The VHA GIS web application has two roles: users and system administrators. Users cannot access PII. Only system administrators can access PII and all must maintain compliance with VA's policies and procedures for elevated privileges, including completion of Privacy and HIPAA Training, VA Privacy and Information Security Awareness Training, Information Security and Privacy Role-Based Training for System Administrators, and signing the VA Information Security Rules of Behavior and Elevated Privileges Rules of Behavior annually.

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 have access to the system and the PII. Contractors provide 95% of the system maintenance and data updates. The written contract includes a confidentiality agreement, non-disclosure agreement, and procedures that must be followed when contractor staff changes occur. At a minimum, the contract is reviewed by the Contracting Officer Representatives, Contracting Specialist, and Contracting Officer annually prior to exercising each option year. It is also reviewed whenever modifications to the contract are made.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All required security related training is available through the VA Talent Management System (TMS).

TMS reports can be pulled at any time via the user or TMS manager access. TMS will send timely notifications to remind users of upcoming required training due. Higher levels of required knowledge/skill are added to System Administrators' competency profiles and role-based training for "those with significant responsibilities" are incorporated into IT Workforce Development Portal for Role-Based Training. System Administrators of the VHA GIS must complete 'Information Security and Privacy Role-Based Training for System Administrators' (TMS#1357076) and review/sign the 'Elevated Privileges Rules of Behavior' annually.

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

If Yes, provide:

- 1. The Security Plan Status,*
- 2. The Security Plan Status Date,*
- 3. The Authorization Status,*
- 4. The Authorization Date,*
- 5. The Authorization Termination Date, .*
- 6. The Risk Review Completion Date*
- 7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

If No or In Process, provide your **Initial Operating Capability (IOC) date**.

An Authority to Operate (ATO) was granted on September 09, 2021. The Authorization Termination Date (ATD) is September 09, 2022.

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, 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.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

The VHA GIS is hosted in the VA Enterprise Cloud Amazon Web Services GovCloud. AWS GovCloud is a FedRAMP high system.

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

The VHA GIS cloud model is Infrastructure as a Service (IaaS)

9.3 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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The contract with the contractors includes a section covering Confidentiality and Non-Disclosure which states that the contractor will have access to some privileged and confidential materials that are for internal use only, not to be copied or released without permission, and remain the sole property of the VA. For specific information, see contract number GS-35F-0490Z, Section A5.0.

In addition, as part of the acquisition process, the VA Privacy Service coordinates with the Office of Operations, Security, and Preparedness (OSP), the Office of Information and Technology (OI&T), and the Office of Cybersecurity, Policy and Compliance (OCS) to include verbiage in the Performance Work Statements and Contract documents including:

- 1) Applicable Documents - a list of the documents with which all contractors shall comply;
- 2) Federal Identity, Credential, and Access Management (FICAM);
- 3) Contractor Personnel Security Requirements;
- 4) Addendum A - Additional VA Requirements, Consolidated;
- 5) Addendum B - VA Information and Information System Security/Privacy Language.

The above requirements are updated with each new contract or contract renewal.

Personnel are required to sign the ROB prior to network or PII/PHI access.

Annual VA training for VHA Privacy and HIPAA training web-based and text versions are available and maintained in TMS.

9.4 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.

The VA Privacy Service is responsible for collecting personally identifiable information (PII) directly from an individual to the greatest extent practicable directly from the subject individual when the information results in adverse determinations about an individual's rights, benefits, and privileges under Federal programs. Privacy Impact Assessment for the VA IT System called: VA Enterprise Cloud (VAEC) Enterprise Cloud Solutions Office (ECSO) Date PIA signed: 7/6/2019 Section 1. Characterization of the Information Section 2. Uses of the Information.

9.5 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.

VA Privacy Service coordinates with the Office of Operations, Security, and Preparedness (OSP), the Office of Information and Technology (OI&T), and the Office of Cybersecurity, Policy and Compliance (OCS) for establishing privacy roles, responsibilities, and access requirements for contractors and service providers, and include privacy requirements in contracts and other acquisition related documents. Contractors take privacy training and sign the Rules of Behavior (ROB) before gaining access to VA networks and information in support of contracts.

9.6 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).

The VHA Geographic Information System does not utilize Robotics Process Automation or Artificial Intelligence.

Section 9. References

Summary of Privacy Controls by Family


Summary of Privacy Controls by Family

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


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

Signature Responsible Officers


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

RITA K GREWAL 114938  Digitally signed by RITA K GREWAL
114938
Date: 2021.11.18 08:40:51 -05'00'

Privacy Officer, Rita Grewal

Andrea B. Mayo 354438  Digitally signed by Andrea B. Mayo
354438
Date: 2021.11.18 07:57:54 -05'00'

Information System Security Officer, Andrea Mayo

Nancy J Kreier 1100500  Digitally signed by Nancy J Kreier
1100500
Date: 2021.11.17 16:08:51 -05'00'

Information System Owner, Nancy Leathers