Privacy Impact Assessment for the VA IT System called:

Vet Equitable Resource Allocation (VERA)

Allocation Resource Center,

Veterans Health Administration (VHA)

eMASS #1459

Date PIA submitted for review:

11/20/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Philip Cauthers*	*Phillip.Cauthers@va.gov*	*503-721-1037*
Information System Security Officer	*James Alden*	*James.Alden@va.gov*	*781-687-4779*
Information System Owner	*Caren Christopher*	*Caren.Christopher@va.gov*	*828-257-3692*

Abstract

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

Supplemental to its essential function of assisting Congress in making funding decisions for the Veterans Health Administration (VHA), Veterans Equitable Resource Allocation (VERA) allocates approximately $110 billion in medical care funding to 18 Veterans Integrated Services Networks (VISNs).

This tool is not a traditional Office of Information Technology (OIT)-developed application, but rather a collection of databases with a reporting website developed by VHA full-time employees, for the Office of the VHA Chief Financial Officer. This tool is internal facing to VA and components reside wholly within the VA and Department of Defense domain.

VERA facilitates pricing that reflects the unique Veteran needs of each Veterans Integrated Services Network (VISN). VISN allocation is based on a combination of the number of patients, adjustments for regional variances in labor and contract costs, high-cost patients, education support, research support and equipment. Every time a patient receives medical care this data is saved.

Each month this data is compiled and analyzed. Every quarter, as well as every year, biannually and every five years, this data is used for both short term and long-term planning. The VERA process is utilized by VHA Office of Finance to compute prices designed to fund major groupings of patients at the network level.

VERA is utilized by 129 medical care facilities, and reporting is available to approximately 400,000 employees. This serves approximately 9,000,000-10,000,000 Veterans per year. VERA processes 140,000 encounters per year and requires the retention of up to 10 years' worth of data. VERA is mandated by Public Law 104-204 to exist and operate. Housed in the Temple, Texas Data Center (CTX), VERA's two servers contain approximately 55 terabytes combined.

Overview

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

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

Veterans Equitable Allocation Resource (VERA), Allocation Resource Center (ARC)

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

Mandated by Public Law 104-204 to exist and operate, this tool allocates approximately $110 billion in medical care funding to 18 Veteran Integrated Service Networks (VISNs). Supplemental to its essential function of assisting Congress in making funding decisions for the VHA, VERA facilitates pricing that reflects the unique Veteran needs of each VISN. VISN allocation is based on a combination of the number of patients, adjustments for regional variances in labor and contract costs, high-cost patients, education support, research support and equipment. Every time a patient receives medical care, this data is saved.

Each month this data is compiled and analyzed. Every quarter, as well as every year, biannually and every five years this data is used for both short term and long-term planning. The VERA process is utilized by VHA Office of Finance to compute prices designed to fund major groupings of patients at the network level.

VERA is utilized by 129 medical care facilities, and reporting is available to approximately 400,000 employees. This serves approximately 9,000,000-10,000,000 Veterans per year.

C. Who is the owner or control of the IT system or project?

VA Owned and Operated (Business-Led IT System).

2. Information Collection and Sharing

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

VERA serves between 9,000,000-10,000,000 Veterans annually. Any Employee, Veteran or Authorized Dependent with a medical history housed within VA has information stored in this system; the typical client is anyone from the aforementioned set of demographics who is seeking medical treatment services in the VHA or affiliated domain.

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

Mandated by Public Law 104-204 to exist and operate, this tool allocates approximately $110 billion in medical care funding to 18 Veterans Integrated Services Networks (VISNs). Supplemental to its essential function of assisting Congress in making funding decisions for the VHA, VERA facilitates pricing that reflects the unique Veteran needs of each VISN. VISN allocation is based on a combination of the number of patients, adjustments for regional variances in labor and contract costs, high-cost patients, education support, research support and equipment. Every time a patient receives medical care, this data is saved.

The database is developed from the Patient Treatment File, National Patient Care Database, Fee Basis Medical and Pharmacy System, Decision Support System (DSS) National extracts, DSS Derived Monthly Program Cost Report (MPCR), Resident Assessment Instrument (RAI)

Minimum Data Set (MDS), Clinical Case Registry (CCR), and Home Dialysis Data Collection System, the Pharmacy Benefits Management database and the Consolidated Enrollment File. Veterans Health Information Systems and Technology Architecture (VistA) feeds the clinical and cost data to the Austin Information Technology Center (AITC). The ARC retrieves this data from the AITC nightly update as needed. Some additional information is received from the Hines Pharmacy Benefits Management and the CCR databases. The data from these sources is combined to develop patient-specific care and cost data for each hospitalization or visit at the location or treatment level. Aggregate tables summarize this data for reporting and analysis purposes. The VERA databases are the basis for resource allocation in the Veterans Health Administration.

Below are specific examples of information collected to support the VA daily operations and Congressional/internal VA reporting functions expressed in the abstract.

Patient Information:

Patient clinical information such as Diagnosis, DRG, CPTs and ICD Procedure Codes
Clinic and Bed Service
Provider & Patient Type (Taxonomy) Information
Dates of Service
Disability Classification
Patient Classification

Facility Information:

Facility Name
Facility Address
Facility/Station Number (STA3N)
Clinic Number (STA6C)
Parent Station Number
Bed Sections

Pharmacy Information:

Facility Number for prescribing facility
Date prescription issued
Unique provider ID for prescribing provider
Unique drug code for the drugs associated with the prescription

NonVA Care (FEE) and Care in the Community Information:

Referencing VA Facility Number
Unique NonVA Provider identifier
Date of treatment
Date of Payment
ICD10 Codes associated with treatment
CPT Codes associated with treatment

DRG Codes associated with treatment
Cost associated with treatment

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

Internally shared with:

Corporate Data Warehouse
Pharmacy Benefits Management
Resident Assessment Instrument/Minimum Data Set (RAI/MDS) Registry

Purpose:

Outpatient, Pharmacy, Purchased Care Claims, MCA National Extracts
Pharmacy prescription information
Long Term Care information
Decision Support System (DSS) costing information
Veteran Enrollment File
Patient classification information

Eternally shared with:

Department of Defense

Purpose:

Inpatient Treatment and costing information for patients treated at VA/DoD joint venture facilities.

G. Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

As stated previously in the abstract, VERA is utilized by the VHA Chief Financial Officer's (CFO) Full Time Employees (FTEs) to assist several mission critical offices and the Department of Defense.

The system is not operated in more than one site.

3. Legal Authority and SORN

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

SORN 121VA10 National Patient Databases –VA, https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: Title 38, United States Code, Section 501.

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The SORN does not require revision or approval. The system does not use cloud technology.

4. System Changes

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

Completion of this PIA will not result in any changes.

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

Completion of this PIA will not result in any technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☐ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone

Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☒ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements:

Patient Information:
Patient clinical information such as Diagnosis, DRG, CPTs and ICD Procedure Codes
Clinic and Bed Service
Provider & Taxonomy Information
Dates of Service
Disability Classification
Patient Classification

Facility Information:
Name
Address
Facility/Station Number (STA3N)
Clinic Number (STA6C)
Parent Station Number
Bed Sections
Parent Station Number
Bed Sections

Pharmacy Information:
Facility Number for prescribing facility
Date prescription issued
Unique provider ID for prescribing provider
Unique drug code for the drugs associated with the prescription

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

Name of drugs associated with the prescription
Quantity/dosage information
Number of refills

Facility Financial Information:
Facility Number
Financial Management System Account Numbers
Staffing Costs
Medical Care Supplies Costs

NonVA Care (FEE) and Care in the Community Information:
Referencing VA Facility Number
Unique NonVA Provider identifier
Date of treatment
Date of Payment
ICD10 Codes associated with treatment
CPT Codes associated with treatment
DRG Codes associated with treatment
Cost associated with treatment

PII Mapping of Components (Servers/Database)

VERA consists of TWO (2) key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VERA and the reasons for the collection of the PII are in the table below.

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

Internal 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
ARC Stage Database	Yes	Yes	Previously Listed in Section 1.1	Formulation of VA Wide Healthcare Budget	• Access Restricted to VA Business Unit personnel • Adherence to VA requirements for endpoint security • Encrypted protocols utilized for data transfers and for communications

					between components
ARC Prod Database	No	Yes	Previously Listed in Section 1.1	Formulation of VA Wide Healthcare Budget	• Access Restricted to VA Business Unit personnel • Adherence to VA requirements for endpoint security • Encrypted protocols utilized for data transfers and for communications between components

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The VERA database is developed from the Patient Treatment File, National Patient Care Database, Fee Basis Medical and Pharmacy System, Decision Support System (DSS) National extracts, DSS Derived Monthly Program Cost Report (MPCR), Resident Assessment Instrument (RAI) Minimum Data Set (MDS), Clinical Case Registry (CCR), and Home Dialysis Data Collection System, the Pharmacy Benefits Management database and the Consolidated Enrollment File.

Veterans Health Information Systems and Technology Architecture (VistA) feeds the clinical and cost data to the Austin Information Technology Center (AITC). The ARC retrieves this data from the AITC nightly update as needed.

Some additional information is received from the Hines Pharmacy Benefits Management and the CCR databases. The data from these sources is combined to develop patient-specific care and cost data for each hospitalization or visit at the location or treatment level.

Aggregate tables summarize this data for reporting and analysis and Congressional reporting purposes.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from

public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Information from sources other than the individual is required primarily to ensure accuracy in data aggregation about patient treatment details, for the purposes of Enterprise-scope resource and funding allocation for all 129 medical facilities. This information is required to be available in real time, and it is required to be accurate; it is not viable to collect from the individual. The information VERA collects is for the purpose of VA operations-related demands and allocations. This ensures integrity and accuracy in reporting for the purposes of Congressionally mandated activities in certain content areas which are to be regularly and continuously analyzed or available for analysis.

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

As already detailed in section 1.2a, the system analyzes information collected elsewhere. It is not a source of information.

To reiterate 1.2a: The database is developed from the Patient Treatment File, National Patient Care Database, Fee Basis Medical and Pharmacy System, Decision Support System (DSS) National extracts, DSS Derived Monthly Program Cost Report (MPCR), Resident Assessment Instrument (RAI) Minimum Data Set (MDS), Clinical Case Registry (CCR), and Home Dialysis Data Collection System, the Pharmacy Benefits Management database and the Consolidated Enrollment File. Veterans Health Information Systems and Technology Architecture (VistA) feeds the clinical and cost data to the Austin Information Technology Center (AITC). The ARC retrieves this data from the AITC nightly update as needed. Some additional information is received from the Hines Pharmacy Benefits Management and the CCR databases.

1.3 How is the information collected?

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

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

The most direct and accurate answer to this brief is: information is collected via data transfers, from VA systems of record. Refer to section 1.1 for specific systems of record. Methods of transfer include: Encrypted transfer using SQL Server Integration Services, Secure FTP (SFTP) data transfer, Encrypted Oracle SQL Net transfer.

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?

VERA information is not collected on the form or subject to the Paperwork Reduction Act.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Information is validated and checked for accuracy by the original systems of record (see 1.1, 1.2) that are responsible for collecting the information from the patients in accordance with VA policies and procedures (see Legal Authority and SORN, above).

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

The system itself does not check for accuracy by accessing a commercial aggregator of information. As the VERA system is a National Level system, it only collects data from National Level Systems of Record. The National Level Systems of Record are populated from the Local Facility Level Systems of Record which in turn collect the data directly from patient encounters.

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

(https://www.oprm.va.gov/privacy/systems_of_records.aspx.

121VA10 National Patient Databases – VA, https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: Title 38 United States Code Section 501.

23VA10NB3 Non-VA Care (Fee) Records, https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf, Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.

24VA10A7 Patient Medical Records-VA, https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf, Title 38, United States Code, Sections 501(b) and 304.

79VA10 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf, Title 38, United States Code, section 7301(a).

121VA10A7 National Patient Databases – VA, https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdf, Title 38 United States Code Section 501.

172VA10 VHA Corporate Data Warehouses-VA, https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf, Title 38, United States Code, Section 501.

CUI
CUI 1 460.02/PEO-20-028 ISA2

INTERCONNECTION SECURITY AGREEMENT BETWEEN DEFENSE HEALTH AGENCY AND VETERANS HEALTH ADMINISTRATION
CONCERNING MILITARY HEALTH SYSTEM INFORMATION PLATFORM AND ALLOCATION RESOURCE CENTER SECURE FILE TRANSFER PORTAL GATEWAYS
DHA 2017-S-297

This is an Interconnection Security Agreement (ISA) between the Defense Health Agency (DHA) and the Department of Veterans Affairs (VA) (together, the "Parties") concerning a bidirectional connection between the DOD Military Health System Information Platform (MIP), owned by DHA, and the VA Allocation Resource Center (ARC) Secure File Transfer Protocol (SFTP) Gateway, owned by VHA. This ISA is required and governed by the Memorandum of Understanding (MOU) between DHA and VHA concerning System-to-System Connectivity, Agreement Number DHA 2017-S-297, and appendices [A and B] identifying the systems whose connection is governed by this ISA. The MOU and Appendix 1 are attached to this ISA as Exhibits A and B (together, the governing MOU). The Parties shall comply with all applicable laws, regulations, directives, instructions and other authorities, including National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach," February 2010; NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," August 2002; and NIST SP 800-53, revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013 (collectively, "applicable authorities"). Each Party reaffirms that its system and the connection between the systems shall be designed, managed, and operated, and each system's data shall be protected, whether at rest, in use or in motion, in accordance with all applicable authorities.

This ISA covers technical details of each system's architecture, the connection between the systems, and each system's connections with other systems, including systems owned and operated by third parties. It documents specific terms of development, management, operation, maintenance, security, and termination of the connection. It defines controls implemented to safeguard the confidentiality, integrity, and availability of the connected systems and the data they store, process, and transmit. It also identifies and appends copies of applicable internal documents, policies, and procedures of each Party, and reconciles any material differences. This ISA is effective upon execution by the appropriate signatories.

Controlled by: PEO DHMS
Controlled by: DHMSM PMO
CUI Category(ies): UNCLASSIFED
Limited Dissemination Control: FEDCON
POC: dha.ncr.budget-resource.mbx.peo-dhms-support-agreements@mail.mil

1. REQUIREMENT FOR CONNECTION AND LIMITATION ON SERVICES

1.1. **PURPOSE**

1.1.1. VA requires the connection for the following purpose or purposes:

☒ Transfer of data from VA ARC SFTP Gateway to DOD MIP

☒ Receipt of data from DOD MIP to be used by all authorized users of SFTP Gateway for the purpose of improving the SFTP's transmittal data type format, frequency, content volume, and automation for managing and reporting outcomes of patient care services

☐ Access to and use of DOD MIP by [all] authorized VA users for the purpose of improving the SFTP's transmittal data type format, frequency, content volume, and automation for managing and reporting outcomes of patient care services.

☐ Confirmation by DOD MIP of receipt of data transferred from VA ARC SFTP Gateway

☐ Other: [Specific purpose]

1.1.2. DHA DAD IO/J-6 requires the connection for the following purpose or purposes:

☒ Transfer of data from DOD MIP to VA ARC SFTP Gateway

☒ Receipt of data from VA ARC SFTP Gateway to be used by all authorized users of DOD MIP for the purpose of improving the SFTP's transmittal data type format, frequency, content volume, and automation for managing and reporting outcomes of patient care services

☐ Access to and use of VA ARC SFTP Gateway by [all] authorized DOD MIP users for the purpose of improving the SFTP's transmittal data type format, frequency, content volume and automation for managing and reporting outcomes of patient care services

☐ Confirmation by VA ARC SFTP Gateway of receipt of data transferred from DOD ARC SFTP Gateway.

☐ Other: [Specific purpose]

1.2. **PROCESS**: Each Party shall ensure that its program or system manager has the capability and means to accomplish, and does accomplish, the actions identified in section 1.1 above in accordance with the terms and conditions of the governing MOU and this ISA.

1.3. **SCOPE AND LIMITATIONS**: This ISA covers only the connection between DOD MIP, which utilizes the Executive Information Decision Support Resource Interface Elements (EI/DS RIE) External Partner Exchange Service (EPES) Server(s) to facilitate many of its data transfers, and VA ARC SFTP Gateway. It does not require either Party to perform user services or other services for the other Party. It does not require or authorize either Party to perform technical services or software changes for the other Party, nor does it require or authorize either Party to bill or pay the other Party

for services. Each Party shall bear the cost of any changes to its system that are necessary to support the connection.

2. SYSTEM AUTHORIZATION: Each Party system shall ensure that its system is authorized to operate, and does operate, in accordance with a valid security authorization. Each Party understands that the other Party's form of certification of authorization depends in part on the authorization process followed by that Party. Appendix A is certification of the current authorizations to operate for DOD MIP, Corporate Executive Information System (CEIS), and EI/DS RIE; and Appendix B is certification of the current authorization to operate for VA ARC SFTP Gateways. Each Party shall maintain its system authorization continuously during the term of this ISA. If either Party does not keep its system authorization current or refuses or ignores requests by the other Party to provide certification of current system authorization, then the requesting Party may suspend the connection after first providing written notice to the other Party and a 30 day opportunity for that Party to produce that certification.

3. SYSTEM SECURITY CLASSIFICATIONS AND SYSTEM-LEVEL CONTINUOUS MONITORING PROCESS

3.1. DOD MIP is authorized to process information up to and including personally identifiable information (PII), Protected Health Information (PHI) and Controlled Unclassified Information (CUI) in the production mode of operation. Information received by DOD MIP from VA ARC SFTP Gateway shall be provided at a level of protection equal to or higher than Public Trust classification in production mode of operation. DHA DAD IO/J-6 shall safeguard and ensure that data in MIP, including data received from VHA ARC SFTP Gateway, is accessed only by authorized personnel with a valid need to know, used only for intended purposes, retains its content integrity, and is marked properly including classification level and handling caveats.

3.2. VA ARC SFTP Gateway is authorized to process information up to and including PII, PHI, and CUI in the production mode of operation. Information received by VA ARC SFTP Gateway from DOD MIP shall be provided at a level of protection equal to or higher than Public Trust. VA shall safeguard and ensure that data in VHA ARC SFTP Gateway, including data received from DOD MIP, is accessed only by authorized personnel with a valid need to know, is used only for intended purposes, retains its content integrity, and is marked properly including classification level and handling caveats.

3.3. Each Party uses a continuous monitoring process with respect to its system security, management, and operational controls in order to maintain security posture awareness of information security, vulnerabilities, and threats, and to facilitate risk-based decision making.

4. DATA

4.1. **TYPES AND ELEMENTS**: Appendix C identifies the data types and data elements to be transmitted from DOD MIP to VA ARC SFTP Gateway, and Appendix D identifies the data types and data elements to be transmitted from VA ARC SFTP Gateway to DOD MIP. Appendices C and D may be updated by written agreement of the Authorizing Official (AO) of each connected system, provided that such updates are necessary and appropriate to meet the objectives of this ISA, maintained with the official files of the ISA, and recorded in the next scheduled annual review of the ISA.

4.2. **SENSITIVITY:** The connection shall carry PII, PHI, and CUI, described in the MOU and subject to the protections and requirements of all applicable authorities.

4.3. **AUTHENTICATION METHODS**: Each Party shall authenticate access to its own system data in accordance with its system security plan, including both identity and credential management methods. Each Party shall provide a copy of its system security plan to the other Party upon request.

4.4. **BACKUP AND STORAGE REQUIREMENTS**: Each Party shall back up and store data in its system in accordance with its system security plan, including any continuity of operations plan,

business continuity plan, and disaster recovery plan, a copy of which shall made be available to the other Party upon request.

5. USERS

5.1. **USER TYPES; USER PROFILES:** All MIP users with access to data received from VA ARC SFTP Gateway are U.S. citizens with a valid and current background investigation or other security clearance, level of trust, or credential as required by DHA DAD IO/J-6. All VA SFTP Gateway users with access to data received from DOD MIP are U.S. citizens with a valid and current background investigation or other security clearance, level of trust, or credential as required by VA. Each Party shall compile and manage user profiles in accordance with the requirements of each agency's Directives and Policies.

5.2. **TRUSTED BEHAVIOR EXPECTATIONS; RULES OF BEHAVIOR**: Each Party expects its system's users to protect data received from the other Party's system in accordance with all app

5.3. **TRAINING; CERTIFICATION; TRACKING AND ENFORCEMENT**: Each Party shall ensure that its personnel and contractors who manage, use, or operate DOD MIP or VA ARC SFTP Gateway and handle CUI, PHI, PII under that Party's supervision, successfully complete annual training in security awareness, security policies, and accepted security practices. Each Party shall track its personnel and contractors' training and professional certifications, strictly enforce its training and certification requirements, and provide proof of compliance to the other Party upon request.

6. INFORMATION EXCHANGE SECURITY: Each Party shall protect the security of the data passed between DOD MIP and VA ARC SFTP Gateway through the use of encryption mechanisms approved by Federal Information Processing Standards Publication 140-2. Each Party developed its system to prevent unauthorized access, modification, destruction, and disclosure of information to unauthorized users. Each Party's system requires user identification and managed credentials for access control. Each Party's system connections are located within controlled access facilities, guarded 24 hours a day. Neither Party shall allow individual user access to data except through security software inherent to its operating system. Each Party shall control all cross-boundary user, application, or system account access by authentication methods made known to the other Party and ensure 100% audit logging of authentication events.

7. SECURITY DOCUMENTATION

7.1. The Parties shall develop, document, and manage system security requirements, and assess and manage system security risks, in accordance with all applicable authorities, including without limitation those identified in the governing MOU.

7.2. The security documentation for VA is known as the VA System Security Plan. The development responsibilities of the document are maintained by the VA ARC SFTP Gateway Information Security Officer (ISO). Security documentation relating to VA ARC SFTP Gateway is stored in an enterprise repository in a secure area. The VA ARC SFTP Gateway ISO shall make relevant security documentation available to the DOD MIP Information System Security Officer (ISSO) for review upon request.

7.3. The security documentation for DOD MIP is known as the DHA DAD IO/J-6 System Security Plan. The development responsibilities of the document are maintained by the DHA DAD IO/J-6 ISSO and approved by the DHA DAD IO/J-6 Information System Security Manager and the DHA DAD IO /J-6 Technology Services Organization Director. Security documentation relating to DOD MIP is stored in the DISA Enterprise Mission Assurance Support Service (eMASS) repository in a secure area. DOD MIP CEIS is classified as a Confidentiality (Moderate), Integrity (Moderate), Availability (Moderate) system and all appropriate security requirements and controls that apply to the system are listed individually in the DHA DAD IO/J-6 Implementation Plan. DHA DAD IO/J-6

addresses best security practices through compliance with the designated Risk Management Framework (RMF) controls for moderate-risk systems. The DOD
MIP ISSO shall make relevant security documentation available to the VA ARC SFTP Gateway ISO for review upon request.
7.4. Appendix E identifies the shared/inherited risk management framework security controls for the connection covered by this ISA.

8. SECURITY INCIDENT RESPONSE AND REPORTING; DISASTER RECOVERY AND REPORTING; OTHER CONTINGENCY PLANS: The Party discovering a security incident shall respond and report it in accordance with applicable authorities and shall provide expedited notice to the other Party in accordance with the governing MOU.

9. PERIODIC INSPECTIONS, COORDINATED TESTING, MATERIAL CHANGES TO SYSTEM CONFIGURATION AND NEW CONNECTIONS: The governing MOU requires that proposed changes to either Party's system or the connecting medium be reviewed and evaluated to determine potential impacts on the connection. It further requires that the Parties renegotiate and amend the ISA before implementing any material change to system configuration. The Parties understand that a change in its system's software, hardware, communications infrastructure, interface procedure, or the format or content of data transferred may constitute a material change. Accordingly, each Party shall conduct periodic inspections of its system to identify reasonably foreseeable change requirements and shall comply with the governing MOU with respect to coordinated testing. Further, each Party shall give the other Party expedited notice and opportunity to assess the risk of material changes to system configurations and new connections in accordance with the governing MOU.

10. TERMINATION PLAN: The Parties shall terminate the connection upon termination of the governing MOU in accordance with the requirements thereof. Either Party may terminate this ISA prior to termination of the governing MOU by giving at least 180 days written notice to the other Party. The Parties may also terminate this ISA at any time upon mutual written consent.

11. AUDIT REVIEW CYCLE AND AUDIT TRAIL: Each Party shall audit and maintain logs of application processes and user activities involving the connection. Each Party shall retain its audit logs for one year and during that time, shall make those logs available to the other Party upon request for investigation, audit and other purposes.

12. TOPOLOGICAL DRAWING/DESCRIPTION: Appendix F illustrates the physical and logical topology of the connection from endpoint to endpoint. It maps all communication paths, circuits, and other components—including firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations—with a level of detail acceptable to both Parties.

13. POINTS OF CONTACT AND LINES OF COMMUNICATION

13.1. Appendix G identifies points of contact (POCs) for communications concerning this ISA. Either Party may change its POCs upon reasonable notice to the other Party.
The named POCs are identified in addition to, not in lieu of, the POCs identified in the governing MOU.

13.2. In accordance with the governing MOU, the Parties shall ensure that their respective POCs maintain open lines of communication with counterpart POCs to support the development, management, operation, security, and termination of each connection, and to safeguard the confidentiality, integrity, and availability of the connected systems and the data they store, process, and transmit.

14. GENERAL TERMS

14.1. **REVIEW**: The Parties shall review this ISA annually on or before the anniversary of its effective date. A copy of each review shall be maintained with this ISA. A sample tracking ledger is attached as Exhibit C.

14.2. **MODIFICATION**: This ISA may be modified only by the written agreement of the Parties, duly signed by their authorized representatives. A copy of each amendment shall be maintained with this ISA. A sample tracking ledger is attached as Exhibit C.
14.3. **DISPUTES**: Any disputes relating to this ISA shall, subject to any applicable law, Executive Order, Directive, or Instruction, be resolved by consultation between the Parties.
14.4. **TRANSFERABILITY**: This ISA is not transferable except with the written consent of the Parties.
14.5. **ENTIRE AGREEMENT**: This ISA embodies the entire agreement between the Parties regarding the ISA's subject matter.
14.6. **EFFECTIVE DATE**: This ISA takes effect beginning on the day after the last Party signs.
14.8. **EXPIRATION DATE**: This ISA expires upon reaching the expiration date of the Governing MOU, which is September 29, 2026.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:

The VERA system will face risks salient to any system that is housed on VA premises and behind VA firewalls with VA security and policy requirements, in accordance with the system's Authority to Operate.

As the VERA system is a national level system, it only collects data from National Level Systems of Record. The National Level Systems of Record are populated from the Local Facility Level Systems

of Record which in turn collect the data directly from the individual patients. VA implements policies and procedures at the Local Facility level to assure accurate, complete, and current information.

Mitigation:

The Veterans Equitable Resource Allocation (VERA) project is careful to only collect the information that has been determined to be required to complete the classification and costing algorithms utilized in the project. By only collecting the minimum necessary information, the project can better protect the Veteran's information. In addition to minimal data collection, the following precautions are also implemented:

General:

All servers involved in the project are running the VA prescribed EndPoint security software.
All servers involved in the project are included in the VA prescribed monthly penetration scanning.
The project **does not** utilize any direct public connections, so is contained within the VA corporate firewall environment and is subject to all VA CSOC and NSOC traffic monitoring and preventative measures.

Data Gathering:

As data is gathered from the various VA systems of record, encrypted protocols such as Secure File Transport Protocol (SFTP) are utilized for the data transfers.

Data Processing Environment:

Access to the data processing environment is restricted to ARC staff only
Logins to the project databases are restricted to ARC staff or approved service accounts only.

Reporting interfaces:

Reports providing PII/PHI data are only served from interfaces that utilize the HTTPS transfer protocol and are secured utilizing certificates issued by the VA's certificate signing authority.
Access to the reporting interfaces that provide PII/PHI is restricted to those VA personnel that have completed the ARC access request for that has to be authorized by the requestor's Facility Director.

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.

The purpose of the VERA system is to combine historical patient treatment and facility financial information with patient treatment and facility financial information for the current fiscal year to

formulate the VA healthcare cost projections for upcoming VA appropriation request submissions to the Office of Management and Budget (OMB) and Congress. The collection of the detailed patient treatment information including the data associated with the treatment of patients at non-VA facilities allows for a higher level of precision in the formulation of the projections for the upcoming submissions.

The data that is contained within the VERA system is also utilized to respond to Congressional inquiries regarding VHA Medical costing and patient classifications.
The VERA data relating to DoD/VA joint venture facilities is shared with DoD to aid DoD's healthcare cost tracking efforts.

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

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

PII/PHI Data Element	Internal Use	External Use
Patient SSN, drug name, fill date, ICD10 diagnosis and procedure codes, DRG, CPT, Date of Service	Outpatient, Pharmacy, Purchased Care Claims, MCA National Extracts	Not used
Patient SSN, drug name, fill date	Pharmacy prescription information	Not used
Patient SSN, Resources Utilization Guidelines (RUG) scores and assessment dates.	Long Term Care information	Not used
Patient SSN, ICD10 diagnosis and procedure codes, CPT, Date of Service	Decision Support System (DSS) costing information	Not used
Patient SSN, date of birth, date of death, gender, ZIP, enrollment date	Veteran Enrollment File	Not used
Patient SSN, patient classification.	Patient classification information	Not used

PII/PHI Data Element	Internal Use	External Use
SSN, div, record type, admit date, treating specialty date of admission, treating specialty date of discharge, treating	Not used	Department of Defense Inpatient Treatment and costing information for

specialty, DRG, treating specialty DRG, CP, DISP, PL DISP, Source of Admission, number of diagnosis codes, diagnosis code 1, diagnosis code 2, diagnosis code 3, diagnosis code 4, diagnosis code 5, Number of non-OR procedures, non-OR procedures, number of OR procedures, OR procedures		patients treated at VA/DoD joint venture facilities

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

Supplemental to its essential function of assisting Congress in making funding decisions for the VHA, VERA facilitates pricing that reflects the unique Veteran needs of each VISN (see abstract above for definition). VISN allocation is based on a combination of the number of patients, adjustments for regional variances in labor and contract costs, high-cost patients, education support, research support and equipment. Every time a patient receives medical care, this data is saved.

As aforementioned, the database is developed from the Patient Treatment File, National Patient Care Database, Fee Basis Medical and Pharmacy System, Decision Support System (DSS) National extracts, DSS Derived Monthly Program Cost Report (MPCR), Resident Assessment Instrument (RAI) Minimum Data Set (MDS), Clinical Case Registry (CCR), and Home Dialysis Data Collection System, the Pharmacy Benefits Management database and the Consolidated Enrollment File. Veterans Health Information Systems and Technology Architecture (VistA) feeds the clinical and cost data to the Austin Information Technology Center (AITC). The ARC retrieves this data from the AITC nightly update as needed. Some additional information is received from the Hines Pharmacy Benefits Management and the CCR databases. The data from these sources is combined to develop patient-specific care and cost data for each hospitalization or visit at the location or treatment level. Aggregate tables summarize this data for reporting and analysis purposes. The VERA databases are the basis for resource allocation in the Veterans Health Administration.

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.

While the system does not create or make available any information about an individual, unique identifiers are collected and linked to the patient's overall encounter with the VHA medical facility to track details like medications, treatment categories, instances of repeat treatment; essentially any detail that would assist the VHA Office of Finance in performing resource allocations and also verify traceability that the data generated is genuine. This does NOT affect any individual in any way, adverse or otherwise; the information is only used for the purpose of verifying tangibility in resource allocation.

2.3 How is the information in the system secured?

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

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

Data Gathering: As data is gathered from the various VA systems of record, encrypted protocols such as Secure File Transport Protocol (SFTP) are utilized for the data transfers. Reporting interfaces: Reports providing PII/PHI data are only served from interfaces that utilize the HTTPS transfer protocol and are secured utilizing certificates issued by the VA's certificate signing authority.

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

As most of the data in the Veterans Equitable Resource Allocation (VERA) project is SSN based, it is all treated as SSN level data and is protected in the way outlined in the mitigation section of section **1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information** of this document.

Secure FTP (SFTP) data transfer through an established secure pipeline between the VA and DoD that requires the identification of the server IP addresses on both the VA and DOD side and utilizes an encrypted tunnel established between the VA and DoD Corporate firewalls.

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

Data is encrypted in transit and encrypted at rest.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Data Processing Environment:
Access to the data processing environment is restricted to ARC staff only
Logins to the project databases are restricted to ARC staff or approved service accounts only.
ServiceNow/SNOW/YourIT tickets are required for the creation of a user account on the project data processing server and for its databases.
ServiceNow/SNOW/YourIT tickets must come from ARC Management staff or the ARC Admin Officer.
ServiceNow/SNOW/YourIT tickets that do not come from the ARC Management staff or the ARC Admin Officer are communicated with the ARC Management staff and are filled or rejected at their discretion.
Reporting interfaces:
Access to the reporting interfaces that provide PII/PHI is restricted to those VA personnel that have completed the ARC access request form. This has to be authorized by the requestor's Facility Director.
Authorization to VERA PII/PHI reports is at the discretion of the requestors Facility Director after they have reviewed the request.
Authorization to VERA PII/PHI is renewed on an annual basis.
Access to VERA PII/PHI is automatically suspended if it is not utilized for a 90-day period.
Reactivation of suspended access to VERA PII/PHI data requires reauthorization by the requestor's Facility Director.

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

Yes.

2.4c Does access require manager approval?

Yes.

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

Yes.

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

Regarding the Office of Information Technology (OIT), the Information System Owner is responsible. However, from the VERA perspective, VERA is run and managed by the office of the Chief Financial Officer; therefore, the Business Owner manages safeguards.

Section 3. Retention of Information

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

3.1 What information is retained?

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

The ARC retains all information that it gathers for 10 years.

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. **The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.** If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Information for the Veterans Equitable Resource Allocation (VERA) project is retained for a period of 10 fiscal years from the end of the fiscal year it was first processed. They are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, General Records Schedule, 5.2, item 020.

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

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

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

The Allocation Resource Center (ARC) is working with their local Records Officer to collect the required documentation to get the current retention schedule submitted to both the VA Records Office and National Archives and Records Administration (NARA) to obtain an office retention schedule.

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

The data in VERA falls under SORN 121VA10 National Patient Databases-VA which has disposition authority approved by the Archivist of the United States, General Records Schedule, 5.2; item 020.

grs05-2.pdf (archives.gov)

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.

The Veterans Equitable Resource Allocation (VERA) project utilizes electronic data files and database tables for its processing. No paper files are utilized by the project. Electronic data files are manually purged from the data processing server by the ARC staff as they determine that the processing of the data files has completed successfully, and the data files have met their requirements for reprocessing and answering ad-hoc data requests. Tables are manually purged from the database by the database administrators as they expire, in accordance with the schedule established with ARC Management.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with

VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.
https://www.va.gov/vapubs/search_action.cfm?dType=1"

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.

Where feasible, VERA uses techniques to minimize the risk to privacy by using PII for research, testing, or training. That process is described below.

No users outside of the owning Business Unit are allowed access to the processing environment or database. VERA is used for the purpose of Congressional budgeting exercises, for resource allocation across 129 VA medical facilities, 19 VISNs, and for other budgeting and resource allocation purposes in multiple Business Offices across VA.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Privacy Risk:

During its multiple decades of operation, the Business Unit has determined that the current 10-year retention of the data allows the VERA system to make the required projection, allows for modification/update planning, maintains the historical data that has already been presented to Congress, and allows the Business Unit to respond to new Congressional Inquiries. There is a risk that information held longer than is necessary may be accessible for an unauthorized use.

Mitigation:

All VERA data is stored in electronic format in database or analytic cubes. When data in the databases reaches its prescribed retention period it is purged from the database and the released space is reutilized for storage of new data. The analytics cubes are re-built monthly and only contain the data prescribed for the reporting period

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
AITC	Inpatient, FEE Basis, FMS, PAID Information	Patient SSN, ICD10 diagnosis and procedure codes, DRG, CPT, Date of Service	Encrypted transfer using SQL Server Integration Services
Corporate Data Warehouse	Outpatient, Pharmacy, Purchased Care Claims, MCA National Extracts	Patient SSN, drug name, fill date, ICD10 diagnosis and procedure codes, DRG, CPT, Date of Service	Encrypted transfer using SQL Server Integration Services
Pharmacy Benefits Management	Pharmacy prescription information	Patient SSN, drug name, fill date	Secure FTP (SFTP) data transfers
RAI/MDS Registry	Long Term Care information	Patient SSN, RUG scores and assessment dates.	Encrypted Oracle SQL Net transfer
MCAO	Decision Support System (DSS) costing information	Patient SSN, ICD10 diagnosis and procedure codes, CPT, Date of Service	Secure FTP (SFTP) data transfers
Chief Strategy Office	Veteran Enrollment File	Patient SSN, date of birth, date of death, gender, ZIP, enrollment date	Secure FTP (SFTP) data transfers
Office of Productivity, Efficiency & Staffing (OPES)	Patient classification information	Patient SSN, patient classification.	Secure FTP (SFTP) data transfers

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Privacy Risk:

The Veterans Equitable Resource Allocation (VERA) project transfers patient treatment and costing data identified in section 5.1 of this document for the four DoD/VA joint venture facilities located across the country. This data allows DoD to calculate their own costs for treating veterans at those facilities and merge DoD costs with VA costs to reach a total cost to treat those patients. This data is transferred from the VERA project due to the facts regarding the collection and compiling of disparate data that was identified in section 4 of this document where DoD does not currently have direct access to all the identified data sources. For DoD to gain access to each of the data sources identified would open one or more potential security and privacy risks for each of the data sources, require additional extracts from each of the identified data sources, and require the establishment of additional data transfers between the VA and DoD.
Breach of the data transfer between the VERA project and the Defense Health Agency (DHA) at DoD would expose treatment and costing information only for those patients that have been treated at one of the four DoD/VA joint venture facilities associated with the data transfer.

Mitigation:

In addition to the efforts outlined in sections 2.3 and 2.4 of this document:
• All systems of record where data is collected from are within the VA's corporate firewall environment and are subject to all VA CSOC and NSOC traffic monitoring and preventative measures
• Only encrypted data transfer protocols are utilized to transfer the data from the identified systems of record
• As the systems where data is collected from are official VA systems of record, they are most likely operating under their own Authorities To Operate (ATO) and are being required to meet the current VA security standards to maintain an ATO.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Department of Defense	Inpatient Treatment and costing information for patients treated at VA/DoD joint venture facilities	SSN, div, record type, admit date, treating specialty date of admission, treating specialty date of discharge, treating specialty, DRG, treating specialty DRG, CP, DISP, PL DISP, Source of Admission, number of diagnosis codes, diagnosis code 1, diagnosis code 2, diagnosis code 3, diagnosis code 4, diagnosis code 5, Number of non-OR procedures, non-OR procedures, number of OR procedures, OR procedures	CUI CUI 1460.02/PEO-20-028 ISA2 Interconnection Security Agreement between Defense Health Agency and Veterans Health Administration concerning military health system information platform and Allocation Resource Center Secure Transfer Portal gateways, DHA 2017-S-297	Secure FTP (SFTP) data transfer through an established secure pipeline between the VA and DoD that requires the identification of the server IP addresses on both the VA and DOD side and utilizes an encrypted tunnel

				establishd between the VA and DoD Corporate firewalls

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

Privacy Risk:

The Veterans Equitable Resource Allocation (VERA) project transfers patient treatment and costing data identified in section 5.1 of this document for the four DoD/VA joint venture facilities located across the country. This data allows DoD to calculate their own costs for treating veterans at those facilities and merge DoD costs with VA costs to reach a total cost to treat those patients. This data is transferred from the VERA project due to the facts regarding the collection and compiling of disparate data that was identified in section 4 of this document where DoD does not currently have direct access to all the identified data sources. For DoD to gain access to each of the data sources identified would open one or more potential security and privacy risks for each of the data sources, require additional extracts from each of the identified data sources, and require the establishment of additional data transfers between the VA and DoD.
Breach of the data transfer between the VERA project and the Defense Health Agency (DHA) at DoD would expose treatment and costing information only for those patients that have been treated at one of the four DoD/VA joint venture facilities associated with the data transfer.

Mitigation: In general:

• The Defense Health Agency (DHA) at DoD is operating on a DoD Authority to Operate (ATO) with security requirements equivalent to those of the VA ATO process
• The transfer of data is done with the Secure File Transfer Protocol (SFTP) data transfer methodology
• The link between the VA server and the DoD server that handles the data transfer utilizes an encrypted Virtual Private Network (VPN) tunnel that has been established between the VA and DoD corporate environments under national level Memorandums of Understanding (MOU) and is controlled and monitored on each end by each agency's respective CSOC group.
• The link is tied to server specific IP addresses at each end of the connection
• Data transfers are only initiated from the VA side of the connection

More details of the connection are contained if the following embedded Interconnection Security Agreement between Defense Health Agency and Veterans Health Administration.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

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

The Veterans Equitable Resource Allocation (VERA) project does not collect information directly from individuals treated by the VA. The VERA project collects data from established VA systems of record. Some of the systems of record that the VERA project collects data from are fed from other VA systems of record that have direct patient interaction (Ex: The Corporate Data Warehouse (CDW) is fed from the VA Veterans Health Information Systems and Technology Architecture [VistA] systems).

Those VA systems of record that do interact directly with the patient adhere to VA and Federal requirements for the notification to individuals before the collection of information. A Privacy

Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

This Privacy Impact Assessment (PIA) also serves as notice 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."

A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority, and the conditions under which the information can be disclosed.

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

The Veterans Equitable Resource Allocation (VERA) project does not collect information directly from individuals treated by the VA. The VERA project collects data from established VA systems of record. Some of the systems of record that the VERA project collects data from are fed from other VA systems of record that have direct patient interaction (Ex: The Corporate Data Warehouse (CDW) is fed from the VA Veterans Health Information Systems and Technology Architecture [VistA] systems).

Those VA systems of record that do interact directly with the patient adhere to VA and Federal requirements for the notification to individuals before the collection of information. A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority, and the conditions under which the information can be disclosed.

Notice was provided and can be found here:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

The VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

This Privacy Impact Assessment (PIA) also serves as notice 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."

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.

Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them.

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.

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR. Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

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 and the local facilities 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. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records. The NOPP is also available at all VHA medical centers from the facility Privacy Officer. The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be***

listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

Any information collected by VERA is obtained from other primary VA Systems of Record. The Notice of Privacy Practices instructs individuals on how they may request their medical records. There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has 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 the medical facility's Release of Information (ROI) office.
VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

However, this query is not salient to VERA as this system is not an external facing system available to any entity or individual outside of VA/DoD operations.

Individuals seeking information on the existence and content of records maintained under SORN 121VA10 that pertains to them should contact the system manager in writing as indicated above or write or visit the VA facility location where they normally receive their care. A request for access to records must contain the requester's full name, address and telephone number, be signed by the requester and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

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)?

System is exempt from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

System is exempt from the access provisions of the Privacy Act.

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.

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 SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. 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.

The Veterans Equitable Resource Allocation (VERA) project does not collect information directly from individuals treated by the VA. The VERA project collects data from established VA systems of record. Some of the systems of record that the VERA project collects data from are fed from other VA systems of record that have direct patient interaction (Ex: The Corporate Data Warehouse (CDW) is fed from the VA Veterans Health Information Systems and Technology Architecture [VistA] systems). Those VA systems of record that do interact directly with the patient adhere to VA and Federal requirements for procedures associated with the correcting of inaccurate or erroneous patient information.

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

Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office.

Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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.

N/A

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Privacy Risk: There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: The risk of incorrect information in an individual's records is mitigated by authenticating information when possible. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments. The NOPP discusses the process for requesting an amendment to one's records.

The Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.
The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA 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?

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?

Access to the data processes environment requires a SNOW ticket from ARC management. Access to the SSN specific reports requires completion of SSN request form on the ARC web site.

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?

There are no users from other agencies with 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 system is accessed by Managers (read and aggregate), VA FTEs (report-only) and Administrators (read, aggregate, maintain).

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.

At this point in time, The Veterans Equitable Resource Allocation (VERA) project does not utilize VA contractors for its operations and if it should begin to, the contractors would not have access to PII.

VA requires mandatory privacy and security training for all employees and contractors that access the information system.

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

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

All users of VERA must complete the standard Privacy, Risk and Rules of Behavior trainings all VA employees must complete to enter and utilize the VA Intranet.

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

8.4a If Yes, provide:

1. *The Security Plan Status: Approved 7/24/2023.*
2. *The System Security Plan Status Date: 9/29/2023*
3. *The Authorization Status: Approved*
4. *The Authorization Date: 9/27/2023*
5. *The Authorization Termination Date: 3/27/2024*
6. *The Risk Review Completion Date: 9/13/2023*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): HIGH*

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

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

N/A

Section 9 – Technology Usage

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

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

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

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

VERA does not utilize the Cloud.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

VERA does not utilize the Cloud.

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.

VERA does not utilize the Cloud.

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.

VERA does not utilize the Cloud.

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).

VERA does not utilize the Cloud or "bots".

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 provided in this Privacy Impact Assessment is true and accurate.

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2024.01.09 12:07:48 -08'00'

Privacy Officer, Philip Cauthers

JAMES B. ALDEN 201589

Digitally signed by JAMES B. ALDEN 201589
Date: 2024.01.09 17:13:58 -05'00'

Information Systems Security Officer, James Alden

CAREN CHRISTOPHER

Digitally signed by CAREN CHRISTOPHER
Date: 2024.01.09 17:24:52 -05'00'

Information Systems Owner, Caren Christopher

APPENDIX A-6.1

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

The VHA Notice of Privacy Practice (NOPP) https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

SORN 121VA10 National Patient Databases –VA, https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

HELPFUL LINKS:

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

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

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

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

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