Privacy Impact Assessment for the VA IT System called:

Enterprise Veterans Health Information Systems and Technology Architecture (Enterprise VistA)

Software Product Management (SPM)

Veterans Health Administration

eMASS ID 946

Date PIA submitted for review:

3/1/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phllip.Cauthers@va.gov	(503) 721-1037
Information System Security Officer (ISSO)	Anita Feiertag	Anita.Feiertag@va.gov	(513)-289-8116
Information System Owner	Scott Madsen	Scott.Madsen@va.gov	(801) 842-3467

Abstract

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

The Department of Veterans Affairs uses the Veterans Health Information Systems and Technology Architecture, better known as VistA, an Electronic Health Record (EHR) system that provides an integrated inpatient and outpatient electronic health record for VA patients, and administrative tools to help VA deliver the best quality medical care to Veterans. VistA is used in all Veteran's Health Administration (VHA) hospitals, medical centers, and outpatient clinics, forming an interconnected EHR that makes a veteran's VA medical record accessible throughout the main VHA facility and connected clinics where the EHR is maintained.

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 Health Information Systems and Technology Architecture (VistA) owned by Software Product Management (SPM).

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

VistA supports a large variety of clinical settings. Facilities range from small clinics that provide solely outpatient care to large medical centers with significant inpatient populations and their associated specialties. The VistA modules focus on clinically relevant record keeping that improves patient care by improving clinical and administrative decision making.

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

VA Owned and VA Operated)

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?

Enterprise VistA comprises over 700,000 Veteran records utilized across VHA at more than 1,500 sites of care, supporting Veterans Affairs Medical Centers (VAMC), Community Based Outpatient Clinics (CBOC) and Community Living Centers (CLC), as well as at nearly 300 VA Vet Centers

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

The types of information include Protected Health Information (PHI) and Personally Identifiable Information (PII) data such as Demographics, Primary Contact, Medical/Mental Health, Criminal Background Information, Guardian, Benefits and Education. Information is collected to ensure veterans and their families receive the benefits and care that they have earned

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

Internal and external information sharing are conducted by VistA. Enterprise VistA consist of 128 VistA instances with 4 data centers. Enterprise VistA is utilized across VHA at more than 1,500 sites of care, supporting Veterans Affairs Medical Centers (VAMC), Community Based Outpatient Clinics (CBOC) and Community Living Centers (CLC), as well as at nearly 300 VA Vet Centers. Enterprise VistA serves America's Veterans by supporting exceptional- quality health care. The VistA modules support a multitude of areas including medical and mental health treatment, medical imaging, supply management, decision support, medical research, and education

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?*

The Veterans Health Information Systems and Technology Architecture (VistA) is a comprehensive, full-featured Health Information System and Electronic Health Record (EHR) owned by the Veterans Affairs Office of Information Technology (OIT). VistA supports a large variety of clinical settings. Facilities range from small clinics that provide solely outpatient care to large medical centers with significant inpatient populations and their associated specialties. The VistA applications focus on clinically relevant record keeping that improves patient care by improving clinical and administrative decision making. VistA Accreditation boundary consists of the VistA instances within aligned Districts. VistA is deployed across VHA at more than 1,500 sites of care, supporting Veterans Affairs Medical Centers (VAMC), Community Based Outpatient Clinics (CBOC) and Community Living Centers (CLC), as well as at nearly 300 VA Vet Centers. VistA serves America's Veterans by supporting exceptional-quality health care. Applications within VistA support a multitude of areas including medical and mental health treatment, medical imaging, supply management, decision support, medical research, and education. The purpose of the system is to collect, create, and maintain data about our VA employees, volunteers, business partners, and Veterans. The types of information include Personal Health Information (PHI) and Personally Identifiable Information (PII) data such as Demographics, Primary Contact, Medical/Mental Health, Criminal Background Information, Guardian, Benefits and Education. The Department of Veterans Affairs (VA) conducts a variety of information sharing both internal and external. Internal sharing is generally done to ensure that veterans and their families receive the benefits and care that they have earned. This system is authorized by 38 United States Code (USC) 7301(a).

3. Legal Authority and SORN

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The following Systems of Record Notices (SORN) apply to information contained in Enterprise VISTA:

24VA10A7. “Patient Medical Records-VA”
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: 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
Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

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?*

System is not in the process of being modified. The SORN will not require amendment, revision, or approval. Enterprise VistA is on prem and 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?*

No, completion of PIA will not result in circumstances that require changes to business processes

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

No, the completion of this PIA cannot result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. 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's Identifier (EDIPI)/Patient ID, Background review information, family relations, Death certificate information, Date of Death, Theater of war, Diagnosis code, Procedure codes, admission type/date, Care-visit date, discharge date, Most recent date of care, medical information, Treating/discharge specialty, Global Assessment of Functioning score via the Mental Health Form, Hospital Visits, Pre-diagnostic health data, Patient care and Treatment data, current procedure/test, Lab results, vital signs, allergies, allergy assessments, appointment date/time, Ward name, Bed name, Attending Physician, admitting Diagnosis, facility name/station, rated disabilities, veterans service information, health insurance beneficiary numbers, benefit information, previous medical records, service connection, service connected disabilities, employment information, employer name/zip code, charges, payments, claims processing, Biller Name/CPAC Biller Name, Account receivable information, Debt collection information, VA claims information, Medication, Provider/Physician name, Patient dispensing record, Rx number, Type of medication, Quantity, instruction of use, Prescription VAMC name/address/phone number, accession number, Blood type, any specimen-specific information such as type of specimen, laboratory results, Study Details including Study Description, Series Details, Images Details, Modality-Specific Details, Post-processing and annotations, radiologist orders, prior reports, and radiology interpretations, System Log files, cache log files, images, text file, Start and End Timestamps, Date of Audit, IP Address of Machine Where User is Logged In Query Action, Employee Name & VistA menu options such as CPRS, ORLs, C&P Exams.

PII Mapping of Components (Servers/Database)

Enterprise VistA consists of 72 key components (servers/databases/instances/applications/software/ application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Enterprise VistA and the reasons for the collection of the PII are in the table below.

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

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
TRAC	**Yes**	**Yes**	Patient Name, VA Master internal Entry Number (IEN)r Person Index (MPI) Integration Control Number (ICN), SSN, Date of Birth (DOB), Sex, Diagnosis codes, Procedure codes, Admission Type, Date of care - Visit Date, Discharge Date, Most Recent Date of Care, Facility Name & Station #, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Insurance, Billing data to include (charges, payments, claims processing, etc.) Medications, Provider Name, Biller Name	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
ONTRAC	**Yes**	**Yes**	Patient Name, Internal Entry Number (IEN), SSN, Date of Birth (DOB), Sex, Diagnosis codes,	Electronic Health Record (EHR) and administrative functions to include	Access control, configuration management, media protection, system and

			Procedure codes, Admission Type, Date of care -Visit Date, Discharge Date, Most Recent Date of Care, Facility Name & Station #, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Insurance, Billing data, Medications, Provider Name, Biller Name	employee and contractor data	service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
Veterans Services Database	**Yes**	**Yes**	Patient Name, IEN, SSN, DOB, Sex, email address, Phone numbers, Employer name/phone #, Diagnosis codes, Procedure codes, Admission Type, Date of care -Visit Date, Discharge Date, Most Recent Date of Care, Facility Name & Station #, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Insurance, Billing data, Medications, Provider Name, Biller Name	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information

Enterprise Denials Database	**Yes**	**Yes**	Patient Name, IEN, SSN, DOB, Sex, email address/Phone numbers, Employer name/phone #, Diagnosis codes, Procedure codes, Admission Type, Date of care -Visit Date, Discharge Date, Most Recent Date of Care, Facility Name & Station #, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Insurance, Billing data, Medications, Provider Name, Biller Name	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
Payer Compliance Server & Payer Compliance Test Database	**Yes**	**Yes**	Patient SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Type, Date of care -Visit Date, Discharge Date, Most Recent Date of Care, Facility Name & Station #, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Insurance, Billing data to include (charges, payments, claims processing, etc.) Medications & Provider	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication,

					physical and environmental protection, system information
Consolidated Mail Out Pharmacy (CMOP) Centralized Database (CDB)	**Yes**	**Yes**	Veteran's pharmaceutical prescription information is retained. Patient's name, address, SSN, RX number, type of medication, quantity ordered, instructions of use, physician's name, prescribing VAMC name, address, and telephone number.	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
Consolidated Mail Out Pharmacy (CMOP) Production Systems Database	**Yes**	**Yes**	Veteran's pharmaceutical prescription information is retained. Patient's name, address, SSN, RX number, type of medication, quantity ordered, instructions of use, physician's name, prescribing VAMC name, address, and telephone number.	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication

					protection, awareness and training, identification authentication, physical and environmental protection, system information
Consolidated Mail Out Pharmacy (CMOP) Ensemble Database	**Yes**	**Yes**	Veteran's pharmaceutical prescription information is retained. Patient's name, address, SSN, RX number, type of medication, quantity ordered, instructions of use, physician's name, prescribing VAMC name, address, and telephone number.	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
Consolidated Mail Out Pharmacy (CMOP) Cancel Site Database	**Yes**	**Yes**	Veteran's pharmaceutical prescription information is retained. Patient's name, address, SSN, RX number, type of medication, quantity ordered, instructions of use, physician's name, prescribing VAMC name,	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning,

			address, and telephone number.		personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
Health Administration Center (HAC) Database	**Yes**	**Yes**	DOB, Address, Sex, Diagnosis Codes, procedure Codes, Admission date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge, Insurance	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
Health Eligibility Center (HEC) Database	**Yes**	**Yes**	Personally, identifiable information (PII) in the form of demographics such as: name, date of birth, social security numbers, race and gender; transient	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and

			information such as phone numbers and addresses; Individually Identifiable Health Information (IIHI) to include diagnosis, treatment, payment, medication, and laboratory results		accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
Health Revenue Center (HRC) Topeka Database	**Yes**	**Yes**	DOB, Address, Sex, Diagnosis Codes, procedure Codes, Admission date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge, Insurance, Medication	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
Veterans Benefits Administration (VBA)	**Yes**	**Yes**	Employee name & VistA menu options such as CPRS, ORLs, Claims and C&P exams	Electronic Health Record (EHR) and administrative functions to	Access control, configuration management, media protection,

				include employee and contractor data	system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
Veterans Health Administration (VHA); Consolidated Patient Accounts Center (CPAC) Database	**Yes**	**Yes**	Patient Name, SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications, Provider Name, CPAC Biller Name	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information

Veterans Health Administration (VHA); Consolidated Mail Out Pharmacy (CMOP) Database	**Yes**	**Yes**	Patient Name, SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications & Provider Name	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
Veterans Health Administration (VHA); All VistA instances via VistA Read-Only Database	**Yes**	**Yes**	Real-time copy of CPRS data to include: Name, SSN, DOB, Mother's Maiden Name, Personal Mailing Address, Personal Phone Numbers, Personal Fax Number, Personal Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender, Next of	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and

			Kin/Dependent information, Guardian, Electronic Protected Health Information, Military History, Service Connection, Service connected disabilities, Employment information and Death Certificate information		environmental protection, system information
Office of Information & Technology (OI&T); Austin Information Technology Center (AITC) Database	**Yes**	**Yes**	VistA shadow copy, data to include Name, SSN, DOB, Mother's Maiden Name, Personal Mailing Address, Personal Phone Numbers, Personal Fax Number, Personal Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender, Next of Kin/Dependent information, Guardian, Electronic Protected Health Information, Military History, Service Connection, Service-connected disabilities, Employment information and Death Certificate information	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
Office of Information & Technology (OI&T); Veterans	**Yes**	**Yes**	VistA copy, data to include: Name, SSN, DOB, Mother's Maiden Name,	Electronic Health Record (EHR) and administrative	Access control, configuration management, media

Data Integration and Federation Enterprise Platform (VDIF- EP) Database			Personal Mailing Address, Personal Phone Numbers, Personal Fax Number, Personal Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender, Next of Kin/Dependent information, Guardian, Electronic Protected Health Information, Military History, Service Connection, Service connected disabilities, Employment information and Death Certificate information	functions to include employee and contractor data	protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
Master Person Index (MPI) Database	**Yes**	**Yes**	Personally, identifiable information (PII) in the form of demographics such as: name, date of birth, social security numbers, race, and gender; transient information such as phone numbers and addresses; Individually Identifiable Health Information (IIHI) to include diagnosis, treatment, payment, medication, and laboratory results.	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and

					training, identification authentication, physical and environmental protection, system information
Veterans Benefits Administration (VBA); Compensation and Pension Record Interchange (CAPRI) Database	**Yes**	**Yes**	Employee name & VistA menu options such as CPRS, ORLs, Claims and C&P exams	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
Health Revenue Center (HRC) – Topeka; Claims Database	**Yes**	**Yes**	Patient Name, SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security,

					system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Enterprise Testing Service VMWare Database	**Yes**	**Yes**	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Veteran Identity/Eligibility Reporting Database	**Yes**	**Yes**	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures,

					contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; My HealtheVet Database	**Yes**	**Yes**	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Veterans Integrated Registries Platform Database	**Yes**	**Yes**	Patient electronic health record, may include: • Name • Social Security Number • Date of Birth	Electronic Health Record (EHR) and administrative functions to include employee and	Access control, configuration management, media protection, system and service

			• Mailing Address • Zip Code • Phone Number • Email Address • Current Medications • Previous Medical Records • Race/Ethnicity • Theatre of War • Date of Death	contractor data	acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Insurance Capture Buffer Web Database	**Yes**	**Yes**	Web Name, Address, SSN, DOB, and insurance information	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Electronic Data Interchange Database	**Yes**	**Yes**	Personally, Identifiable Information (PII) to	Electronic Health Record (EHR) and	Access control, configuration management,

			include but not limited to Patient Name, Date of Birth and Social Security Number	administrative functions to include employee and contractor data	media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; VEText (Text Message Appointment Reminders)	**Yes**	**Yes**	Patient name, IEN, phone number and appointment date & time	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection,

					system information
VHA; Clinical Data Repository/Health Data Repository Database	**Yes**	**Yes**	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Veterans Data Integration and Federation Enterprise Platform Database	**Yes**	**Yes**	Users login identifier, User ID, Name of User, Patient's Identifier (EDIPI), Query Action - what widgets the user accesses within Veteran EHR, Start and End Timestamps, Date of N Audit, IP Address of Machine Where User is Logged In	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification

					authentication, physical and environmental protection, system information
VHA; Central Fee System	**Yes**	**Yes**	Name, SSN, Date of Birth (DOB), Mailing Address, Zip Code, Financial Account Information, Medical Records, VA claims Information, Healthcare Provider Taxpayer ID (TIN), Health Insurance Beneficiary Numbers, Military Service Data	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Bed Management Solution	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Ward Name Bed Name Race/Ethnicity, Patient VA MPI Integration Control Number (ICN)/Internal Entry Number (IEN)	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication

			Attending Physician Admitting Diagnosis		protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Veterans Point of Service Kiosk	**Yes**	**Yes**	Personally Identifiable Information (PII) to include but not limited to Patient Name, Date of Birth and Social Security Number	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA & VBA; Claims Processing & Eligibility System	**Yes**	**Yes**	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning,

					personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Health Data Repository	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity VA MPI Integration Control Number (ICN)/Internal Entry Number (IEN)	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Joint Legacy Viewer (JLV)	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and

			Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity VA MPI Integration Control Number (ICN)/Internal Entry Number (IEN)		accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; eHealth Exchange	**Yes**	**Yes**	PII to include but not limited to Patient Name, Date of Birth and Social Security Number	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Veterans Personal Finance System	**Yes**	**Yes**	SSN, Full Name, Gender, Date of Birth, Date of Death, Address, Phone Number, Email	Electronic Health Record (EHR) and administrative functions to	Access control, configuration management, media protection,

			Address, Admission Date, Discharge Date	include employee and contractor data	system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Referral Authorization System	**Yes**	**Yes**	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information

VHA; Capacity and Performance Engineering Services	**Yes**	**Yes**	Personally, Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable information is obtained from VistA, to include but not limited to Patient Name, Date of Birth and Social Security Number	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Behavioral Health Laboratories	**Yes**	**Yes**	PII/PHI to include but not limited to Patient Name, Date of Birth and Social Security Number	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification

					authentication, physical and environmental protection, system information
VHA; National Provider Identification Crosswalk	**Yes**	**Yes**	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; VistA Audit Solution	**Yes**	**Yes**	Personally, Identifiable Information (PII), Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security,

					system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Portal for Electronic Third-party Insurance Recovery	**Yes**	**Yes**	Name SSN DOB Mailing Address Zip Code Phone Number(s) Health Insurance Beneficiary Information	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; National Medical Information System	**Yes**	**Yes**	Name, Zip Code, SSN, DOB, Age, Gender, Race/Ethnicity, Patient Treatment information, Current procedure/test, Previous Medical records, Diagnostic codes, Procedure	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and

			codes, Hospital visits, Pre- diagnostic health data.		accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; VistA Imaging	**Yes**	**Yes**	System Log files, cache log files, images, text files, clinical data, etc., PII/PHI to include but not limited to Patient Name, Date of Birth and Social Security Number,	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Community Viewer	**Yes**	**Yes**	Name, Social Security Number Date of Birth Mailing Address Zip Code, Phone	Electronic Health Record (EHR) and administrative	Access control, configuration management,

			Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN Internal Entry Number (IEN)	functions to include employee and contractor data	media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Medical Care Cost Recovery (MCCR) – National Database (NDB)	**Yes**	**Yes**	Name, Account receivables information, Debt Collection information, billing information	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection,

					system information
VHA; 3D Wound Care Management Solution	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Abbott Point of Care Portal	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/ Internal Entry Number (IEN)	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and

					training, identification authentication, physical and environmental protection, system information
VHA; Accu-Chek 360	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN Internal Entry Number (IEN)	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Anesthesia Record Keeper	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning,

					personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Caribou CLC Suite	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address, Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Data Access Services	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address	Electronic Health Record (EHR) and administrative functions to include employee and	Access control, configuration management, media protection, system and service

			Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/ Internal Entry Number (IEN)	contractor data	acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Epic Cadence Enterprise Scheduling	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/ Internal Entry Number (IEN)	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Logicare	**Yes**	**Yes**	Name	Electronic Health Record	Access

			Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN, Internal Entry Number (IEN)	(EHR) and administrative functions to include employee and contractor data	control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Patient Advocate Tracking System	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication,

					physical and environmental protection, system information
VHA; Praedico	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; PraediGene	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and

					communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Veterans Service Network	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Clinical Assessment, Reporting and Tracking	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability

			Previous Medical Records Race/Ethnicity Patient ICN/IEN		measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; IAM - Single Sign-On Internal	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; IAM - Provisioning	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address	Electronic Health Record (EHR) and administrative functions to	Access control, configuration management, media

			Zip Code Phone Number(s) Email Address Emergency Contact Information	include employee and contractor data	protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; VDIF Disruptive Behavior Reporting System	**Yes**	**Yes**	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records, Race/Ethnicity Patient ICN/IEN	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection,

					system information
VHA; eScreening	**Yes**	**Yes**	Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Surgery Risk Assessment Database	**Yes**	**Yes**	Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and

					training, identification authentication, physical and environmental protection, system information
VHA; Standards and COTS Integration Platform (formerly BHIE)	**Yes**	**Yes**	Query parameters for clinical information containing the patient ID (VA Integration Control Number (ICN)) and the type of clinical data being requested such as Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc.), service information, medical information, and benefit information	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Laboratory System Reengineering PathNet	**Yes**	**Yes**	PII as needed for specimen identification – SSN, Date of Birth, Sex, Race, Name, Blood Type, any specimen-specific information such as type of specimen	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning,

					personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Healthcare Claims Processing System	**Yes**	**Yes**	Patient Name, SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications.	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; VBECS Med	**Yes**	**Yes**	PII as needed for specimen identification – SSN, Date of Birth, Sex, Race, Name, Blood Type, any specimen-specific information	Electronic Health Record (EHR) and administrative functions to include employee and	Access control, configuration management, media protection, system and

			such as type of specimen	contractor data	service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information
VHA; Mental Health Suite	**Yes**	**Yes**	Patient demographic data, to include Global Assessment of Functioning scores via the Mental Health Form	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information

VistA Audit Solution (VAS)	**Yes**	**Yes**	Name, Social security, Date of Birth (DOB), personal mailing Address, Medical record, Personal email address, Personal Phone number, Race and Ethnicity, Health Insurance, Beneficiary Account Numbers, and Financial Records, Emergency Contact Information (Name, Phone Number)	Electronic Health Record (EHR) and administrative functions to include employee and contractor data	Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information

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?

In general, we know that most, if not all VHA facilities will share data with internal VA programs and systems, including at a minimum:

- VA National Cemetery Administration (NCA)
- Veterans' Benefit Administration (VBA)
- Consolidated Mail Out Pharmacy (CMOP)
- Consolidated Patient Accounts Center (CPAC
- Veteran's Benefit Administration (VBA)
- Health Eligibility Center (HEC)
- Health Revenue Center (HRC)
- Austin Information Technology Center (AITC)

Data, such as confirmation of military service or results of employee background checks, come from external Federal Agencies. These agencies include at a minimum:

- Department of Defense (DOD); Defense Health Agency (DHA)

- Internal Revenue Service (IRS)
- Office of Personnel Management (OPM)
- Social Security Administration (SSA)
- Federal Emergency Management Agency (FEMA)
- Federal Bureau of Investigation (FBI)

External sharing varies on a facility-by-facility basis and may for example share with the State Prescription Monitoring Program (SPMP), Research Partners, Departments of Health and private medical institutions.

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 veterans, their dependents, VA employees, VA contractors, members of the public or individuals are not required.

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

The system functions as the source of information and creates information such as analysis and reports.

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?

Information collected from individuals is collected verbally in interviews and conversations with VA medical and administrative staff, in writing (such as on VA Form 10-5345, Request for and Authorization to Release Medical Records Fillable), and via electronic and web form submissions. Information is also collected from a variety of other IT systems and resources internal and external to the VA. These data collections may be completed using secure web portals and VPN connection.

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?

OMB control number: 2900-0260 and various VA Forms.

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

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

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

The VHA facility where the PII is collected is responsible for confirming the timeliness, completeness, check and correct inaccurate or outdated PII continuously or on as needed basis in reference to the organizations collection and creation of PII.

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

No, the system does not check for its information accuracy by accessing a commercial aggregate of information, each VHA facility where the PII is collected is tasked with the responsibility of checking and making sure information is accurate.

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

Enterprise VistA and all VHA facilities' VistA instances operate under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b) and 304, and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The following Systems of Record Notices (SORN) apply to information contained in Enterprise VistA:

> 24VA10A7. "Patient Medical Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: 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
> Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191(Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).

Additional information about state laws, local policies, and more can be found by reviewing the individual Area Privacy Impact Assessments (PIAs). https://department.va.gov/privacy/system-of-records-notices.

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: Enterprise VistA contains sensitive personal information – including social security numbers, names, and protected health information – on veterans, members of the public, & VA employees and contractors. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result.

Mitigation: Veterans Health Administration (VHA), Enterprise VistA, as well as the facilities deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors. Security measures include access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance

Section 2. Uses of the Information

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

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

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

The Veterans Health Information Systems and Technology Architecture (VistA) is a comprehensive, full-featured Health Information System and Electronic Health Record (EHR) owned by the Veterans Affairs Office of Information Technology (OIT). VistA supports a large variety of clinical settings. Facilities range from small clinics that provide solely outpatient care to large medical centers with significant inpatient populations and their associated specialties. The VistA applications focus on clinically relevant record keeping that improves patient care by improving clinical and administrative decision making. VistA Accreditation boundary consists of the VistA instances within aligned Districts. VistA is deployed across VHA at more than 1,500 sites of care, supporting Veterans Affairs Medical Centers (VAMC), Community Based Outpatient Clinics (CBOC) and Community Living Centers (CLC), as well as at nearly 300 VA Vet Centers.

VistA serves America's Veterans by supporting exceptional-quality health care. Applications within VistA support a multitude of areas including medical and mental health treatment, medical imaging, supply management, decision support, medical research, and education. The purpose of the system is to collect, create, and maintain data about our VA employees, volunteers, business partners, and Veterans. The types of information include Personal Health Information (PHI) and Personally Identifiable Information (PII) data such as Demographics, Primary Contact, Medical/Mental Health, Criminal Background Information, Guardian, Benefits and Education. The Department of Veterans Affairs (VA) conducts a variety of information sharing both internal and external. Internal sharing is generally done to ensure that veterans and their families receive the benefits and care that they have earned. This system is authorized by 38 United States Code (USC) 7301(a).

Due to the extensive amount and nature of the information contained at each facility which can determine what information to collect, process, retain, or disseminate, a full understanding of the purpose for each individual data point can be obtained by reviewing the facility-level Privacy Impact. [https://department.va.gov/privacy/system-of-records-notices.](https://department.va.gov/privacy/system-of-records-notices)

The records and information (e.g., Name, Social Security Number, Date of Birth, Mother's Maiden Name, Mailing Address, Zip Code, Phone Number(s), Fax Number, Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers, Certificate/License Numbers, Internet Protocol (IP) Address Numbers, Current Medications, Previous Medical Records, Race/Ethnicity) may be used for statistical analysis to produce various management, workload tracking and follow-up reports; to track and evaluate the ordering and delivery of equipment, services and patient care; the planning, distribution and utilization of resources; the possession and use of equipment or supplies; the performance of vendors, equipment, and employees; and to provide clinical and administrative support to patient medical care.

The data may be used for research purposes. The data may be used also for such purposes as assisting in the scheduling of tours of duties and job assignments of employees; the scheduling of patient treatment services, including nursing care, clinic appointments, surgery, diagnostic and therapeutic procedures; the repair and maintenance of equipment and for follow-up activities to determine that the actions were accomplished and to evaluate the results; to plan, schedule, and maintain rosters of patients, employees and others attending or participating in sports, recreational or other events (e.g., National Wheelchair Games, concerts, picnics); for audits, reviews and investigations conducted by staff of the health care facility, the Network Directors Office, VA Central Office, and the VA Office of Inspector General (OIG); for quality assurance audits, reviews, investigations and inspections; for law enforcement investigations; and for personnel management, evaluation and employee ratings, and performance evaluations.

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
Name	Patient demographics	Not used
Social Security Number	Patient demographics	Not used
Date of Birth	Patient demographics	Not used
Mother’s Maiden Name	Patient demographics	Not used
Personal Mailing Address	Patient demographics	Not used
Personal Phone Number(s)	Patient demographics	Not used
Personal Fax Numbers	Patient demographics	Not used
Personal email Address	Patient demographics	Not used
Emergency Contact Information (Name, Phone number etc. of a different individual)	Patient demographics	Not used
Financial Information	Insurance/Billing data	Not used
Health Insurance Beneficiary Numbers/account numbers	Disability/Eligibility, Health Insurance Beneficiary	Not used
Certificate/License Numbers	Patient demographics	Not used
Internet Protocol (IP) Address Numbers	File identification purposes	Not used
Medications	Pharmacy prescription data	Not used
Medical Records	Patient demographics	Not used
Race/ethnicity	Patient demographics	Not used
Tax Identification Number	Insurance/Billing data	Not used
Medical Record Number	Patient demographics	Not used
Gender	Patient demographics	Not used
Integrated Control Numbers (ICN)	Patient demographics	Not used
Military History/Service Connection	Patient demographics	Not used
Next of kin	Patient demographics	Not used
Other data elements listed (under Section 1.1)	patient demographics, Health information, Facility information, Disability/eligibility, Insurance/Billing data, pharmacy prescription data, Laboratory data, VistA Imaging/Radiology, Employee	Not used

	Audit Trail data, Employee data table	

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?

Patient and employee data are analyzed on an as-needed basis with tools relevant to the task at hand upon official authorization. Tools and applications used to analyze data will vary from facility to facility. Typically, statistics and analysis are utilized to create 3 types of general reports that provide the VA a better understanding of patient care and needs. The reports are:

1. Reports created to analyze statistical analysis on case mixes.
2. Analyze the number of places and geographical locations where patients are seen to assess the volume of clinical need.
3. Track and trend appointment availability and length data to track and trend average wait times.
   Please reference the individual Privacy Impact Assessments for each facility to learn more. https://department.va.gov/privacy/system-of-records-notices.

To learn more about the above software visit https://www.va.gov/vdl/ for a complete list of the nationally released VistA Class 1 software packages.

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.

If the system makes available new or previously unutilized information about an individual, the information is placed into the individuals existing medical record. No action is taken against or for the individual identified because of the newly derived information. Such information is accessible to Government employees with the need-to-know.

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?

VA approved secured connections and encryptions are in place to protect data in transit and at rest.

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

Additional security controls are applied to Enterprise VistA to provide extra layer of protection for PII.

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

Appropriate administrative and technical safeguards are in place to safeguard PII/PHI in Enterprise VistA in accordance with OMB Memorandum *M-05-15* to include making sure all personnel enroll and complete the VA Privacy and Information Security Awareness and Rules of Behavior.

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?

Access to PII is determined based on assigned personnel roles and responsibilities with Enterprise VistA.

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

Criteria, procedures, controls, and responsibilities regarding access to Enterprise VistA PII is documented in the Enterprise VistA Privacy Controls Standard Operating Procedure.

2.4c Does access require manager approval?

Access to Enterprise VistA requires require approvals from both the information Systems Owner (ISO) and Information Systems Security Officer (ISSO).

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

The VA Privacy Service in conjunction with the Senior Agency Official for Privacy (SAOP), the Privacy Compliance Assurance Office, and the Office of Enterprise Risk Management (ERM) monitors, tracks or records access to PII.

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

Entities responsible for assuring safeguards for PII includes VA Privacy services in conjunction with the Senior Agency Official for Privacy (SAOP), the Privacy Compliance Assurance Office, and the Office of Enterprise Risk Management (ERM).

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 records include information concerning current and former employees, applicants for employment, trainees, contractors, sub-contractors, contract personnel, students, providers and consultants, patients and members of their immediate family, volunteers, maintenance personnel, as well as individuals working collaboratively with VA. Below is a list of information that may be retained in the facility VistA instances:

- Name
- Social Security Number
- Date of Birth
- Mother's Maiden Name
- Personal Mailing Address
- Personal Phone Numbers
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Information
- Health Insurance Beneficiary Numbers and Account numbers
- Certificate/License Numbers
- Vehicle License Plate Numbers
- Internal Protocol (IP0 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 PII/PHI data elements:

Patient's Identifier (EDIPI)/Patient ID, Background review information, family relations, Death certificate information, Date of Death, Theater of war, Diagnosis code, Procedure codes, admission type/date, Care-visit date, discharge date, Most recent date of care, medical information, Treating/discharge specialty, Global Assessment of Functioning score via the Mental Health Form, Hospital Visits, Pre-diagnostic health data, Patient care and Treatment data, current procedure/test, Lab results, vital signs, allergies, allergy assessments, appointment date/time, Ward name, Bed name, Attending Physician, admitting Diagnosis, facility name/station, rated disabilities, veterans service information, health insurance beneficiary numbers, benefit information, previous medical records, service connection, service connected disabilities, employment information, employer name/zip code, charges, payments, claims processing, Biller Name/CPAC Biller Name, Account receivable information, Debt collection information, VA claims information, Medication, Provider/Physician name, Patient dispensing record, Rx number, Type of medication, Quantity, instruction of use, Prescription VAMC name/address/phone number, accession number, Blood type, any specimen-specific information such as type of specimen, laboratory results, Study Details including Study Description, Series Details, Images Details, Modality-Specific Details, Post-processing and annotations, radiologist orders, prior reports, and radiology interpretations, System Log files, cache log files, images, text file, Start and End Timestamps, Date of Audit, IP Address of Machine Where User is Logged In Query Action, Employee Name & VistA menu options such as CPRS, ORLs, C&P Exams.

Please reference the facility-level Privacy Impact Assessment to learn more. https://department.va.gov/privacy/system-of-records-notices.

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.*

When managing and maintaining VA data and records, Enterprise VistA, and the VHA facilities will follow the guidelines established in VA Directive 6300, Records and Information Management dated September 2018; VA Handbook 6300.1, Records Management Procedures dated March 24, 2010; VA Directive 6371, Destruction of Temporary Paper Records dated April 2014; VA Directive 6500, VA Cybersecurity Program, NIST SP 800-88 rev 1, Guidelines for Media Sanitization https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf and VA Record Control Schedule (RCS) 10-1 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf). This document specifies how long records will be retained by the VA, if/when they will be transferred to a national records storage location, and the length of time the records will be stored at the national level. For greater details related to records retention, please review VA Handbook6300.1 and RCS 10-1.

Below are some key record retention schedules for your information:

Health Record Folder File or Consolidated Health Record (CHR) contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a VA records storage facility.
Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS) 10-1 6000.1d and 6000.2b (dated January 2021)).

Information Technology Operations and Maintenance Records are retained under (RCS) 10–1, Item 2000.2 and destroyed 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.

System Access Records RCS 10–1, Item 2100.3 2100.3 with disposition authority DAA–GRS–2013–0006– 0004, item 31. These are destroyed 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

Official Human Resources Personnel File: Folder will be transferred to the National Personnel Records Center (NPRC) within 30 days from the date an employee leaves the VA. NPRC will destroy 65 years after separation from Federal service. (Department of Veterans Affairs Record Control Schedule (RCS)10-1, Section 3020 Employee Management Records (GRS 2.2) https://www.archives.gov/files/records-mgmt/grs/grs02-2.pdf (dated April 2022).

Financial Records: Different forms of financial records are retained 1-7 years based on specific retention schedules. Please refer to VA Record Control Schedule (RCS) 10-1 Financial Management Section 4000 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf) for specific guidelines.

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

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

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

All records stored within Enterprise VistA follow the guidelines established in the NARA-approved Department of Veterans' Affairs Record Control Schedule (RCS) 10-1 and General Records Schedule (GRS).

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

VA Medical Records are retained under RCS 10-1 chapter 6, 6000.1d with disposition authority N1–15–91–6, Item 1d and 6000.2b with disposition authority N1–15–02–3, Item 3. Medical record information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted.

Information Technology Operations and Maintenance Records are retained under (RCS) 10–1, Item 2000.2 with disposition authority DAA–GRS–2013–0005– 0004, item 020. These are destroyed 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.

System Access Records are retained under RCS 10–1, Item 2100.3 2100.3 with disposition authority DAA–GRS–2013–0006– 0004, item 31. These are destroyed 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

Official Human Resources Personnel File: NPRC will destroy 65 years after separation from Federal service. (Department of Veterans Affairs Record Control Schedule (RCS)10-1, Section 3020 Employee Management Records (GRS 2.2).

Financial Records: Different forms of financial records are retained 1-7 years based on specific retention schedules. Please refer to VA Record Control Schedule (RCS) 10-1 Financial Management Section 4000 for specific guidelines.

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.

“Electronic data and files of any type, including Protected Health Information (PHI) , Sensitive Personal Information (SPI), Human Resource 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 Recycled 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 " https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf and the VA Media Sanitization User’s Guide (May 05, 2022). 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 based on the VA Media Sanitization User’s Guide.

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.*

All IT system and application development and deployment is handled by VA OIT and authorized contracting staff. VHA does test new or modified IT systems for VHA operations prior to deployment, and PII/PHI may be used for that Alpha or Beta testing at the facility-level per VHA policy. In addition, VHA may need to train staff on functionality in the new or modified application(s). Training, including on IT systems, is part of health care operations and per VHA policy PII and PHI may be used for that training purpose. However, VHA must minimize the use of PII and PHI in training presentations or materials per VA policy. Where feasible, Veterans Affairs will use techniques to minimize the risk to privacy of using PII for research, testing and training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information contained in the Enterprise VistA facility instances will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached

Mitigation: In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary.

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***
TRAC	Designed to manage and track medical equipment, supplies, and possibly pharmaceuticals throughout their lifecycle	Patient Name, VA Master internal Entry Number (IEN)r Person Index (MPI) Integration Control Number (ICN), SSN, Date of Birth (DOB), Sex, Diagnosis codes, Procedure codes, Admission Type, Date of care -Visit Date, Discharge Date, Most Recent Date of Care, Facility Name & Station #, Rated Disabilities/Eligibility, Treating/Discharge Specialty,	(TCP/IP)/RPC Broker/HL7

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***
		Insurance, Billing data to include (charges, payments, claims processing, etc.) Medications, Provider Name, Biller Name	
ONTRAC	Functions as a Logistics and tracking solution with VHA. Designed to optimize the delivery and management of healthcare services. Streamlines operations, improve supply chain efficiency, and ensure timely delivery of medical supplies, equipment and enhance the overall coordination of care.	Patient Name, Internal Entry Number (IEN), SSN, Date of Birth (DOB), Sex, Diagnosis codes, Procedure codes, Admission Type, Date of care -Visit Date, Discharge Date, Most Recent Date of Care, Facility Name & Station #, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Insurance, Billing data, Medications, Provider Name, Biller Name	(TCP/IP)/RPC Broker/HL7
Veteran Services Server	Ensures that veterans receive care and services tailored to their specific needs.	Patient Name, IEN, SSN, DOB, Sex, email address, Phone numbers, Employer name/phone #, Diagnosis codes, Procedure codes, Admission Type, Date of care -Visit Date, Discharge Date, Most Recent Date of Care, Facility Name & Station #, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Insurance, Billing data, Medications, Provider Name, Biller Name	VistA Link/RPC Broker/HL7
Enterprise Denials Server	Used to manage and review denials of claims for veteran benefits and services.	Patient Name, IEN, SSN, DOB, Sex, email address/Phone numbers, Employer name/phone #, Diagnosis codes, Procedure codes, Admission Type, Date of care -Visit Date, Discharge Date, Most Recent Date of Care, Facility Name & Station #, Rated	(TCP/IP)/RPC Broker/HL7

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***
		Disabilities/Eligibility, Treating/Discharge Specialty, Insurance, Billing data, Medications, Provider Name, Biller Name	
Payer Compliance Server & Payer Compliance Test Sever	Enables the identification of systemic patterns that result in incorrect allowable rates based on your contractual agreements with payers	Patient SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Type, Date of care -Visit Date, Discharge Date, Most Recent Date of Care, Facility Name & Station #, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Insurance, Billing data to include (charges, payments, claims processing, etc.) Medications & Provider	(TCP/IP)/RPC Broker/HL7
Consolidated Mail Out Pharmacy (CMOP) Centralized Database (CDB)	Manage and streamline the process of prescribing, filling, and delivering medication to veterans through a mail-order system.	Veteran's pharmaceutical prescription information is retained. Patient's name, address, SSN, RX number, type of medication, quantity ordered, instructions of use, physician's name, prescribing VAMC name, address, and telephone number.	VistA Mailman messaging
Consolidated Mail Out Pharmacy (CMOP) Production Systems	Automate and manage the processing, filling, and shipping of prescriptions medication to veterans	Veteran's pharmaceutical prescription information is retained. Patient's name, address, SSN, RX number, type of medication, quantity ordered, instructions of use, physician's name, prescribing VAMC name, address, and telephone number.	VistA Mailman messaging
Consolidated Mail Out Pharmacy (CMOP) Ensemble System	Enhances the coordination and management of mail-order pharmacy services with VHA. System utilizes advanced software to integrate various processes	Veteran's pharmaceutical prescription information is retained. Patient's name, address, SSN, RX number, type of medication, quantity ordered, instructions of use, physician's name, prescribing	VistA Mailman messaging

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***
	involved in prescription management, including order entry, fulfillment, and shipping.	VAMC name, address, and telephone number.	
Consolidated Mail Out Pharmacy (CMOP) Web Cancel Site	Provides a regional system resource to expedite the distribution of mail-out prescriptions to veteran patients	Veteran's pharmaceutical prescription information is retained. Patient's name, address, SSN, RX number, type of medication, quantity ordered, instructions of use, physician's name, prescribing VAMC name, address, and telephone number.	VistA Mailman messaging
Health Administration Center (HAC)	Overseas the delivery and administration of healthcare services to include managing VA medical facilities, ensuring the quality of care, coordinating patient services, and implementing healthcare policies	DOB, Address, Sex, Diagnosis Codes, procedure Codes, Admission date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge, Insurance	VistA Mailman messaging
Health Eligibility Center (HEC)	Primary system for assigning and maintaining unique person identifiers	Personally, identifiable information (PII) in the form of demographics such as: name, date of birth, social security numbers, race and gender; transient information such as phone numbers and addresses; Individually Identifiable Health Information (IIHI) to include diagnosis, treatment, payment, medication, and laboratory results	Health Level 7 (HL7)
Health Revenue Center (HRC) Topeka	Identifies, manages, and collects patient service revenue	DOB, Address, Sex, Diagnosis Codes, procedure Codes, Admission date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge, Insurance, Medication	Secure Shell (SSH) / Remote Procedure Broker Calls (RPC) broker

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Benefits Administration (VBA)	Offers VBA Rating Specialists help in building the rating decision documentation through online access to medical data	Employee name & VistA menu options such as CPRS, ORLs, Claims and C&P exams	Remote Procedure Control (RPC) broker
Veterans Health Administration (VHA); Consolidated Patient Accounts Center (CPAC)	Combines and put together patients account into a single entity.	Patient Name, SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications, Provider Name, CPAC Biller Name	Secure File Transfer Protocol (SFTP)
Veterans Health Administration (VHA); Consolidated Mail Out Pharmacy (CMOP)	Provides a regional system resource to expedite the distribution of mail-out prescriptions to veteran patients	Patient Name, SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications & Provider Name	VistA Mailman messaging
Veterans Health Administration (VHA); All VistA instances via VistA Read-Only	Provides the ability to access and view data across all instances of VistA.	Real-time copy of CPRS data to include: Name, SSN, DOB, Mother's Maiden Name, Personal Mailing Address, Personal Phone Numbers, Personal Fax Number, Personal Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender, Next	Transmission Control Protocol (TCP) Secure Sockets Layer (SSL)

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*
		of Kin/Dependent information, Guardian, Electronic Protected Health Information, Military History, Service Connection, Service connected disabilities, Employment information and Death Certificate information	
Office of Information & Technology (OI&T); Austin Information Technology Center (AITC)	Hosts on-premises information systems in support of the Veterans Experience. Additionally, the ITC provides backup/recovery and contingency operations for the remaining four ITCs	VistA shadow copy, data to include Name, SSN, DOB, Mother's Maiden Name, Personal Mailing Address, Personal Phone Numbers, Personal Fax Number, Personal Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender, Next of Kin/Dependent information, Guardian, Electronic Protected Health Information, Military History, Service Connection, Service-connected disabilities, Employment information and Death Certificate information.	Transmission Control Protocol (TCP) Secure Sockets Layer (SSL)
Office of Information & Technology (OI&T); Veterans Data Integration and Federation Enterprise Platform (VDIF- EP)	Standards based, healthcare IT integration and interoperability platform. It is a COTS product from Intersystem. It is a single, common middleware platform to service and enable VistA, includes the ability to read, write, and share VistA data.	VistA copy, data to include: Name, SSN, DOB, Mother's Maiden Name, Personal Mailing Address, Personal Phone Numbers, Personal Fax Number, Personal Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Previous	Encryption Control Protocol (ECP) connection

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*
		Medical Records, Race/Ethnicity, Medical Record Number, Gender, Next of Kin/Dependent information, Guardian, Electronic Protected Health Information, Military History, Service Connection, Service connected disabilities, Employment information and Death Certificate information	
Master Person Index (MPI)	Primary system for assigning and maintaining unique person identifiers	Personally, identifiable information (PII) in the form of demographics such as: name, date of birth, social security numbers, race and gender; transient information such as phone numbers and addresses; Individually Identifiable Health Information (IIHI) to include diagnosis, treatment, payment, medication, and laboratory results.	Health Level 7 (HL7)
Veterans Benefits Administration (VBA); Compensation and Pension Record Interchange (CAPRI)	Compensation and Pension Record Interchange (CAPRI) supports Compensation and Pension exam information. The CAPRI software acts as a bridge between VBA and VHA information systems. It offers VBA Rating Specialists help in building the rating decision documentation through online access to medical data.	Employee name & VistA menu options such as CPRS, ORLs, Claims and C&P exams	Remote Procedure Control (RPC) broker
Health Revenue Center (HRC) – Topeka; Claims server	Identifies, manages, and collects patient service revenue	Patient Name, SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility,	Secure Shell (SSH) / Remote Procedure Broker Calls (RPC) broker

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***
		Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications,	
VHA, Enterprise Testing Service VMWare Database	Deliver to Testing Services Engineering and Integration (TSEI) customers a highly scalable, secure and innovative service that allows organizations to seamlessly migrate and extend their on-premises VMware vSphere-based environments to the IV&V Test Center: thereby providing customer access capability to databases hosted at various geographic locations	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	ASCII over SSH, TCP
VHA, Veteran Identity/Eligibility Reporting System	Provide consuming business applications with access to a standard, enterprise view of person demographic, contact, military service and other benefits information.	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	Electronically pulled from VistA thru Computerized Patient Record System (CPRS)
VHA, My HealtheVet	Web-based application that creates a new, online environment where Veterans, family, and clinicians may come together to optimize veterans health care	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	HL7 over MLLP/ Patient data exchanged via electron transmission. MHV

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***
VHA, Veterans Integrated Registries Platform	Provides clinician on-demand reporting capabilities and integrate ad-hoc reporting/query capabilities	Patient electronic health record, may include: • Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number • Email Address • Current Medications • Previous Medical Records • Race/Ethnicity • Theatre of War • Date of Death	Secure Hypertext Transfer Protocol (HTTPS) / Health Level-7 (HL-7
VHA, Insurance Capture Buffer Web	Designed to enhance the insurance data collection and verification processes for Veterans Affairs facilities	Web Name, Address, SSN, DOB, and insurance information	Remote Procedure Call Broker (RPC)
VHA, Electronic Data Interchange	Responsible for the transport of the Veterans health, benefits, or administrative data between consumers and producers	Personally, Identifiable Information (PII) to include but not limited to Patient Name, Date of Birth and Social Security Number	MLLP, AS2, SSH FTP & FTP/s with TLS
VHA, VEText (Text Message Appointment Reminders)	Appointment reminder system. VEText pulls appointment data from VistA and sends an appointment reminder (via third party SMS gateway) to Veteran allowing them to either confirm or cancel their appointment.	Patient name, IEN, phone number and appointment date & time	Electronically pulled from VistA via standard RPCs

VHA, Clinical Data Repository/Health Data Repository	Generates standards-based, computable, electronic health records that can be exchanged between the two agencies healthcare systems for patients marked as Active Dual Consumers (ADC)	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	HL7 over TCP/IP
VHA, Veterans Data Integration and Federation Enterprise Platform	It is a single, common middleware platform to service and enable VistA, includes the ability to read, write, and share VistA data.	Users login identifier, User ID, Name of User, Patient's Identifier (EDIPI), Query Action - what widgets the user accesses within Veteran EHR, Start and End Timestamps, Date of Audit, IP Address of Machine Where User is Logged In	HTTPS
VHA, Central Fee System	Authorizes and pays private physicians, hospitals (in-patient) and pharmacists for products and services dispersed to approved Veterans for non-VA care	Name, SSN, Date of Birth (DOB), Mailing Address, Zip Code, Financial Account Information, Medical Records, VA claims Information, Healthcare Provider Taxpayer ID (TIN), Health Insurance Beneficiary Numbers, Military Service Data	Encrypted electronic message via mailman service in VISTA
VHA, Bed Management Solution	Real-time, user-friendly web-based Veterans Health Information Systems and Technology Architecture (VistA) interface for tracking patient movement, bed status and bed availability within the VA system	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Ward Name Bed Name Race/Ethnicity, Patient VA MPI Integration Control Number (ICN)/Internal Entry Number (IEN) Attending Physician Admitting Diagnosis	VIA VistA Integration Adapter (VIA) / Medical Domain Web Services (MDWS)
VHA; Veterans Point of Service Kiosk	Allow Veterans to do self-check-in for appointments, update demographics and insurance info, perform	Personally Identifiable Information (PII)	HL-7

	Med Reconciliation and Allergy reviews	to include but not limited to Patient Name, Date of Birth and Social Security Number	
VHA & VBA, Claims Processing & Eligibility System	Handles the eligibility and claims payments functions for five Congressionally mandated programs: Civilian Health and Medical Program of the VA (CHAMPVA); CHAMPVA Caregiver; Children of Women Vietnam Veterans (CWVV); Foreign Medical Program (FMP); and Spina Bifida.	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	Via secure file transfer protocol within the VA Network, FIPS 2.0
VHA; Health Data Repository	Used by clinicians and other personnel to facilitate longitudinal patient-centric care	Names, emails, Address, social security numbers, Lab results, Vital Signs, Allergies, Allergy Assessments, and Outpatient Pharmacy Medications	Electronically pulled from VistA thru VAMC thru E-VIE (Enterprise VistA Interface Engine) thru JMS (Java Message Service) Queues thru CDS (Clinical Data Services) Message Mediator
VHA, Joint Legacy Viewer (JLV)	Custom patient-centric, web presentation system that pulls information from disparate health care systems in real-time for presentation in a browser design	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity VA MPI Integration Control Number (ICN)/Internal Entry Number (IEN)	Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS).

VHA, eHealth Exchange	Responsible for the transport of the Veterans health, benefits, or administrative data between consumers and producers	PII to include but not limited to Patient Name, Date of Birth and Social Security Number	HTTPS
VHA, Veterans Personal Finance System	Mini-banking system used by the Veterans Health Administration (VHA) to manage the accounts of VHA patients in the VHA hospital system	SSN, Full Name, Gender, Date of Birth, Date of Death, Address, Phone Number, Email Address, Admission Date, Discharge Date	VistALink
VHA, Referral Authorization System	Enterprise-wide system in support of community care used by facility community care staff to generate referrals and authorizations for Veterans receiving care in the community.	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	HL7
VHA, Capacity and Performance Engineering Services	production system that provides pre-production staging for products in development prior to their release and/or to enable critical development lifecycle actions that require VistA.	Personally, Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable information is obtained from VistA, to include but not limited to Patient Name, Date of Birth and Social Security Number	Fileman SFTP over TCP/IP
VHA, Behavioral Health Laboratories	collect mental health assessment data captured during structured interviews with patients	PII/PHI to include but not limited to Patient Name, Date of Birth and Social Security Number	TCP/IP
VHA, National Provider Identification Crosswalk	National Provider Identification Crosswalk	Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	Inbound HL7 - Outbound Mailman
VHA, VistA Audit Solution	Provides a nationwide HIPAA compliant Audit Tracking Solution with the ability to track and report on access logs for patient's PII/PHI data across all VistA instances.	Personally, Identifiable Information (PII), Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number	FIPS 140-2 Encrypted TCP

VHA, Portal for Electronic Third-party Insurance Recovery	A system used by the VHA to streamline the process of identifying, billing, and collecting payments from third party insurance providers for healthcare services provided to veterans.	Name SSN DOB Mailing Address Zip Code Phone Number(s) Health Insurance Beneficiary Information	HL7 message exchange using TCP/IP protocol
VHA, National Medical Information System	Comprehensive system utilized by VHA to manage and store electronic health record (EHR) and other medical information for veterans.	Name, Zip Code, SSN, DOB, Age, Gender, Race/Ethnicity, Patient Treatment information, Current procedure/test, Previous Medical records, Diagnostic codes, Procedure codes, Hospital visits, Pre-diagnostic health data.	Mailman to the AITC z13 mainframe NMIS application queues
VHA, VistA Imaging	Picture Archiving and Communication System (PACS) system that is the mandated Primary Storage Record for all VHA patient Administrative and Clinical Images	System Log files, cache log files, images, text files, clinical data, etc., PII/PHI to include but not limited to Patient Name, Date of Birth and Social Security Number	RPC Calls or web services over HTTPS using TLS version 1.2 encryption.
VHA, Community Viewer	Managing referrals for internal care and community care	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN Internal Entry Number (IEN)	Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS).
VHA, Medical Care Cost Recovery (MCCR) – National Database (NDB)	Functions as a system that collects and analyzes data related to the costs of medical provided to veterans. It supports the process of identifying, billing, and recovering healthcare costs from third-party insurance companies, other responsible parties,	Name, Account receivables information, Debt Collection information, billing information	Mailman

	or the veterans themselves when applicable		
VHA, 3D Wound Care Management Solution	Allow clinicians to more consistently and accurately measure and document wounds, collaboratively monitor healing progress with other care team members, standardize treatment protocols, and better manage and prioritize wound care patients through analytical dashboard and proactive alerts.	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	Electronically transmitted to/from VistA thru Computerized Patient Record System (CPRS) via RPC Broker and VistA Imaging via RPC Broker + Background Processor via Samba share
VHA, Abbott Point of Care Portal	Digital platform used to manage and access diagnostic testing information from A abbot point-of-care testing devices.	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/ Internal Entry Number (IEN)	HL7 over TCP/IP
VHA, Accu-Chek 360	Designed to collect self-care data and analyze results with comprehensive graphs and reports that will act on the results to continually improve diabetes management	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN Internal Entry Number (IEN)	RPC Broker
VHA, Anesthesia Record Keeper	Help clinicians manage large volumes of data in the operating room by assembling important data and providing a	Name Social Security Number Date of Birth Mailing Address Zip Code	HL7 over TCP/IP

	complete overview of a patient's status at any point in time.	Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity	
VHA, Caribou CLC Suite	Provides a comprehensive and standardized assessment of each residents functional capabilities	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	TCP/IP VSOA config.xml file.
VHA, Data Access Services	Responsible for the transport of the Veterans health, benefits, or administrative data between consumers and producers	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/ Internal Entry Number (IEN)	RPC Broker
VHA, Epic Cadence Enterprise Scheduling	Provides veterans with modernize and timely access of care	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/ Internal Entry Number (IEN)	HL7 V2 over HTTPS via the HAPI standard
VHA, Logicare	provides information regarding treatments, diagnosis, procedures, follow-up instructions, lifestyle changes,	Name Social Security Number Date of Birth Mailing Address Zip Code	HL7 over TCP/IP

	applicable medications, and community resources	Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN, Internal Entry Number (IEN)	
VHA, Patient Advocate Tracking System	captures Interactions between Veterans or their beneficiaries and Patient Advocates through multiple channels	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information	RPC query-VistALink
VHA, Praedico	Monitoring infectious disease outbreaks, public health surveillance activities, veteran influenza reporting, and look-back and epidemiological investigations	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	SFTP/SSH
VHA, PraediGene	Veteran health issues and infectious disease outbreaks.	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	SFTP/SSH
VHA, Veterans Service Network	Designed to manage the administration of healthcare and services to veterans. Each Veteran Service Network oversees a specific geographic area, coordinating and	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address	VistA Link/RPC Broker/HL7

	ensuring the provision of comprehensive healthcare services through VA medical centers, outpatient clinics and other facilities within its jurisdiction	Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	
VHA, Clinical Assessment, Reporting and Tracking	Monitor and enhance the quality and safety of medical specialty care for Veterans through clinical analytics and information technology	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	RPC Broker
VHA, IAM - Single Sign-On Internal	enhance the user experience by reducing time associated with multiple logon/logoff activities, enriched password management, and reduction in help desk support	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	VistA Link/RPC Broker/HL7
VHA, IAM - Provisioning	Provides capabilities to create system accounts for users throughout the VA user lifecycle	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information	VistA Link/RPC Broker/HL7
VHA; VDIF Disruptive Behavior Reporting System	Designed to track and manage incidents of disruptive behavior by patients with VA healthcare facilities. The system allows staff to report, document, and address behaviors that	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address	xml SOAP

	can compromise the safety of patients, staff and visitors, ensuring a safe and therapeutic environment for all	Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	
VHA; eScreening	Automate collection and scoring of screening instruments to improve efficiency in treating patients	Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	RPC Broker/Mail Man
VHA, Surgery Risk Assessment Database	Assessments of selected surgical operations performed at Veteran Affairs Medical Centers (VAMCs)	Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information	HL7
VHA; Standards and COTS Integration Platform (formerly BHIE)	Facilitates inter and intra-agency data sharing within Department of Veterans Affairs (VA) and with the Department of Defense (DoD) in support of patient care, Veteran engagement, claims processing and benefits adjudication	Query parameters for clinical information containing the patient ID (VA Integration Control Number (ICN)) and the type of clinical data being requested such as Veteran or Primary Subject’s Personal Contact Information (name, address, telephone, etc.), service information, medical information, and benefit information	Electronically sent via a CPRS RDV remote procedure call to STA200 and returned via an RDV response
VHA, Laboratory System Reengineering PathNet	Focused on patient-centric reporting and correcting patient safety issues.	PII as needed for specimen identification – SSN, Date of Birth, Sex, Race, Name, Blood Type, any specimen-specific information such as type of specimen	HL7 via TCP/IP
VHA; Healthcare Claims Processing System	Used by VHA to manage and process healthcare claims. It facilitates the efficient handling of billing and reimbursement for healthcare services provided to veterans including the submission	Patient Name, SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications	HL7 via TCP/IP

	of claims to third party insurers		
VHA; VBECS Med	Automate the daily processing of blood inventory and patient transfusions in a hospital transfusion service. facilitates ongoing compliance with Food and Drug Administration (FDA) standards for medical devices and enhances the Veterans Health Administration's (VHA's) ability to produce high-quality blood products and services to veterans	PII as needed for specimen identification – SSN, Date of Birth, Sex, Race, Name, Blood Type, any specimen-specific information such as type of specimen	HL7 via TCP/IP
VHA, Mental Health Suite	Support the development and documentation of multidisciplinary treatment plans	Patient demographic data, to include Global Assessment of Functioning scores via the Mental Health Form	HL7 via TCP/IP
VistA Audit Solution (VAS)	provides a nationwide HIPAA compliant Audit Tracking Solution with the ability to track and report on access logs for patient's PII/PHI data across all VistA instances	Name, Social security, Date of Birth (DOB), personal mailing Address, Medical record, Personal email address, Personal Phone number, Race and Ethnicity, Health Insurance, Beneficiary Account Numbers, and Financial Records, Emergency Contact Information (Name, Phone Number)	FIPS 140-2 Encrypted TCP

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The sharing of data is necessary for the medical care of individuals eligible to receive care at a VHA facility. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance. The access request process utilizing Electronic Permission Access System (eMASS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

The use of a Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two-factor authentication.

VistA menus and security keys are assigned by an approved access request based on specific job or duty requirements with least privileges. This access is reviewed for appropriateness on a bi-annual basis. VistA applies the sensitive record flag to all employee and any veteran record where the veteran requests the record be sensitized. The ISSO reviews VistA audit messages for any potential access abnormalities or violations.

VA Facilities complete a multitude of auditing functions based on VA Handbook 6500 guidelines. VA Facilities complete an in-depth audit of VistA accounts to include separated users, elevated privileges, file access, separation of duties, sensitive records, inactive accounts as well as adhoc reports upon request.

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***
Cerner Corporation	Implementation of a modern electronic health record (EHR) system across VHA	Data consists of PII, and PHI with information such as patient name, DOB, SSN, veteran service information, family relation, and medical information.	National MOU/ISA	Health Level 7 (HL7), HL7 Optimized (HLO) via Site to Site (S2S) Virtual Private Network (VPN) tunnel
Department of Defense	Sharing of medical and logistics data to Military Health Systems	Patient Care & Treatment Data Logistics Data to support Patient Care	MedCOI MOU/ISA	Joint Network Protection Suite (J- NPS) and Local Enclave Interconnection
Department of Defense	Sharing of medical and logistics data to Military Health Systems	Patient Care & Treatment Data to support Patient Care	MedCOI MOU/ISA	Bi-directional Health Information Exchange
Integrates with VistA modules to provide a full	Provide full Electronic Health Record (EHR) services	Name, SSN, DOB, Mother’s Maiden Name, Personal Mailing Address, Personal Phone Numbers,	MedCOI MOU/ISA	Health Level 7 (HL7), Secure File Transfer Protocol

service Electronic Health Record (EHR)		Personal Fax Number, Personal Email Address, Emergency Contact Information, Financial Account Information, Beneficiary Numbers/Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender, Next of Kin/Dependent information, Guardian, Electronic Protected Health Information, Military History, Service-Connection, Service-connected disabilities,		(SFTP), Transmission Control Protocol/Internet Protocol (TCP/IP)
VHA; Cerner Health Intent	Helps identify and stratify risk across the veteran population, optimize care delivery, and manage the health of veterans more proactively.	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/IEN	MedCOI MOU/ISA	HL7 over TCP/IP
Each State's Prescription Monitoring program	Enhance patient safety by monitoring and managing the prescription of controlled substances	Patient Demographics, Patient Full Social Security Number (SSN), Patient Date of Birth (DOB), Patient Dispensing Record, Facility Information, Patient Unique ID	In accordance with Title 38 (Code of Federal Regulations) CFR Part 1	Secure File Transfer Protocol (SFTP), Secure Shell (SSH) key authentication
Lab Corps	Electronic data Interchange of receipt of laboratory orders, result and reporting delivery	Patient Demographics, Social Security Number (SSN), Patient Date of Birth (DOB), Accession Number, Current procedure/test, Blood Type, any specimen-specific information such as type of specimen, Laboratory results.	MOU-ISA - National	HL7/S2S VPN
Quest Diagnostics	Utilizes laboratory testing services to enhance diagnostic capabilities with VHA	Patient Name, DOB, Sex, Patient ID, Accession Number, VA facility code, client or account number, order codes and names, any comments associated with the orders, any specimen source or type	MOU-ISA-National	S2S VPN

		required, result codes and names, laboratory testing results.		
LSRP (Laboratory System Reengineering Project)	Enhances Laboratory operations through the adoption of advanced technologies, process improvement, and system integrations.	Patient name, date of birth (DOB), Social Security Number (SSN), veteran service information, family relation, and medical information. Records can be retrieved using full name, SSN, and financial account number. Records can also be retrieved via searches on accession number, Medical Record Number, birth date, and gender	MOU/ISA-National	TCP/IP
Central Tox	Enables VHA to conduct comprehensive toxicology screening and analysis, essential for diagnosing and managing cases involving substance abuse, exposure to toxins, and poisoning.	Patient Demographics only include Name, Medical Record Number, Date of Birth, coded in a HL7 format for Patient Test orders and results messages.	MOU-ISA-National	SSL/TLS
LEDI & Oracle	Streamlines the process of sending and receiving laboratory test orders and results between VA healthcare facilities and external laboratories or partners.	Both PII and PHI data will be transmitted over this dataflow direction. Elements include information such as patient name, date of birth (DOB), Social Security Number (SSN), veteran service information, family relation, and medical information. Records can be retrieved using full name, SSN, and financial account number. Records can also be retrieved via searches on accession number, Medical Record Number (MRN), birth date, and gender	Oracle Cerner Vista (LEDI) MOU ISA 1.0	MLLP/(TCP/IP)

The Valor Network System (VNS)	Designed to enhance the management and coordination of healthcare services with VHA	Patient Details including, Patient Name, Patient ID, Date of Birth, Accession Number. Study Details including, Study Description. Series Details, Images Details, Modality-Specific Details and Post-processing and annotations, Electronic Protected Health Information (ePHI), Radiologist orders, prior reports, and radiology interpretations	MOU-ISA - National	HL7 / S2S VPN

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: The sharing of data is necessary for the medical care of individuals eligible to receive care at a VHA facility. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

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 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.
Additionally, the Department of Veterans Affairs provides additional notice of this system by publishing two System of Record Notices (SORNs):

- The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10A7 (Oct 2nd, 2020), in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

- The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10 (Dec 23rd, 2020), in the Federal Register and online. An online copy of the SORN can be found at https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.

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."

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

Notices are provided as listed in response to 6.1a above.

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

The Notice of Privacy Practice (NOPP) is a document that explains the collection and use of protected information to individuals applying for VHA benefits. Major changes are mailed out every three years to all VHA beneficiaries. Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on an annual basis.

The SORNs (24VA10A7 and 79VA10) are published to the Federal Register and are visible accessible to the public on the internet.

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.

The Veterans' Health Administration (VHA) as well as the individual facilities request only information necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information to the VHA, this will prevent them from obtaining the benefits necessary to them.

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with the VA.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

VHA permits individuals to agree to the collection and to the consent to the use of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. If the individual does not want their information collected or used, then they do not sign the consent form.

In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices (NOPP) and conversations with VHA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required.

Where legally required VHA obtains signed, written authorizations from individuals prior to releasing, disclosing, or sharing PII and PHI. Individuals have a right to restrict the disclosure and use of their health information. Individuals have a right to deny the use of their health information and/or IIHI and for the purpose of research. Individuals can request further limitations on other disclosures. A veteran, guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information. The facility can approve or deny these requests. However, if the request to provide information is accepted, the facility must conform to the restrictions.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

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

<u>Privacy Risk:</u> 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.

<u>Mitigation:</u> This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries on a yearly basis and periodic monitoring is performed to check that the signed acknowledgment form has been scanned into electronic records. Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) 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.***

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.

Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative (COR) to obtain information upon request.

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)?

The system is not 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?

The system functions as a Privacy Act System, procedures and regulations in place covers individuals gaining access to his or her information is covered under 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.

Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative (COR) to correct inaccurate or erroneous information upon request.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

Veterans and other individuals are encouraged to use the formal redress procedures discussed in question 7.3 above to request edits to their personal medical records and other personal records retained about them.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that a Veteran does not know how to obtain access to their records or how to request corrections to their records and that the health record could contain inaccurate information and subsequently effect the care the Veteran(s) receive.

Mitigation: As discussed in question 7.3, the Notice of Privacy Practice (NOPP), is provided to all enrolled Veterans which discusses the process for requesting an amendment to ones' records.
The VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their medical 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 to obtain access to all the available features.

In addition, Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

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 is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information System Security Officer (ISSO), local Area Manager (AM), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information. Access is requested per VA policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor and OIT approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes.

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?

Access to users from other agencies is requested per VA policies utilizing Electronic Permission Access System (ePAS). Users submit access request based on need to know and job duties, the same guidelines apply to what PII can be shared.

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.

Roles created to provide access to the system include Information Systems Security Officer (ISSO), Local Area Manager (AM), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive information. Each role has clearly defined responsibilities that grants the individual access to information needed to perform his or her duties.

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.

Contracts are reviewed based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee).
Per specific contract guidelines, contractors/subcontractors are authorized to use VA information systems or access to VA information in accordance with VA Handbook 6500.6, Contract Security Privacy Checklist. The appropriate background investigation must be initiated, and fingerprinting conducted. All users of VA information systems or VA information must complete required training, VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176). The user must accept the Rules of Behavior (ROB) to indicate that they have read, understood, and agree to abide by the ROB before access is provided to the VA information system or the VA information. Authorized users must complete and comply with this training on an annual basis.

Privacy and HIPAA training (VA 10203) must be completed for access to ePHI. Certification that this training has been completed by all contractors must be provided to the VHA employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy.
Contractors with VistA access must have an approved electronic access request on file and access reviewed with the same requirements as VHA employees.

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 VA employees who have access to VA information must complete the onboarding and annual mandatory Department-wide privacy and information security training. In addition, all employees who interact with patient sensitive medical information must complete the VA mandated privacy HIPAA training. Finally, all new employees receive face-to-face training by the facility Privacy Officer and Information System Security Officer (ISSO) during new employee orientation. The Privacy and ISSO also perform subject specific trainings on an as needed basis.

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

8.4a If Yes, provide:

1. The Security Plan Status: Completed (Approved)
2. The System Security Plan Status Date, February 08, 2023
3. The Authorization Status: Two (2) -Year ATO
4. The Authorization Date, -------------- July 07, 2023
5. The Authorization Termination Date, -------- July 05, 2025
6. The Risk Review Completion Date: ----- July 03, 2023
7. The FIPS 199 classification of the system, 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.***

Authorization and Accreditation (A&A) has been completed for the system. Details provided in 8.4a.

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)*

Enterprise VistA functions as an on prem system and does NOT use cloud technology. Therefore, the requested cloud details do not apply to Enterprise VistA.

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.*

Enterprise VistA functions as an on prem system and does NOT use cloud technology. Therefore, the requested cloud details do not apply to Enterprise VistA

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.

Enterprise VistA functions as an on prem system and does NOT use cloud technology. Therefore, the requested cloud details do not apply to Enterprise VistA

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.

Enterprise VistA functions as an on prem system and does NOT use cloud technology. Therefore, the requested cloud details do not apply to Enterprise VistA

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).

Enterprise VistA functions as an on prem system and does NOT use cloud technology. Therefore, the requested cloud details do not apply to Enterprise VistA

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

Digitally signed by PHILLIP CAUTHERS
Date: 2024.03.11 14:38:24 -07'00'

Privacy Officer, Phillip Cauthers

ANITA FEIERTAG

Digitally signed by ANITA FEIERTAG
Date: 2024.03.12 11:07:00 -04'00'

Information Systems Security Officer, Anita Feiertag

SCOTT MADSEN

Digitally signed by SCOTT MADSEN
Date: 2024.03.12 09:17:53 -06'00'

Information Systems Owner, Scott Madsen

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).

VHA Notice of Privacy Practices
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

SORN 24VA10A7. “Patient Medical Records-VA”
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

SORN 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

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 Directive 1605.04: Notice of Privacy Practices