Date PIA submitted for review:

August 18, 2021

Privacy Impact Assessment for the VA Area Boundary called[1]:

Area White River Junction (WRJ)

North Atlantic

Facilities Supported by the Area

Facilities Supported by the Area:
1) White River Jct. VA Medical Center (VAMC)
2) White River Jct. Regional Office (VBA)

[1] The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, Area Boundary, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

3) Bennington VA Clinic
4) Brattleboro VA Clinic
5) Burlington Lakeside VA Clinic
6) Keene VA Clinic
7) Littleton VA Clinic
8) Newport VA Clinic
9) Rutland VA Clinic
10) Berlin Vet Center
11) Keene Outstation (Vet Center)
12) South Burlington Vet Center
13) White River Jct. Vet Center

Area Boundary Contacts:

Area Privacy Officer

Name	**Phone Number**	**Email Address**	**Location**
Designated Area PO (The PO located in the same VAMC as the Area Manager): Joseph Smeraldi	802-369-4606	Joseph.Smeraldi@va.gov	White River Jct.

Area Information System Security Officer

Name	Phone Number	Email Address	Area Boundary Site
Joseph Friesenhahn	802-296-6305	Joseph.friesenhahn@va.gov	White River Jct.

Area Manager

Name	Phone Number	Email Address	Area Boundary Site
Matthew Rafus	802-291-6288	Matthew.Rafus@va.gov	White River Jct.

Legend:

Abstract

The abstract provides the simplest explanation for "what does the area boundary do?" and will be published online to accompany the PIA link.

VA White River Jct. Healthcare System is an Information Systems Boundary that consists of the White River Jct. VA Medical Center, Bennington VA Clinic, Brattleboro VA Clinic, Burlington Lakeside VA Clinic, Keene VA Clinic, Littleton VA Clinic, Newport VA Clinic, Rutland VA Clinic, Berlin Vet Center, Keene Outstation (Vet Center), South Burlington Vet Center, White River Jct. Vet Center and the White River Jct. Regional Office (VBA). The systems environment is comprised of workstations, laptops, portable computing devices, terminals, servers, printers, and IT enabled networked medical devices and special purpose systems. The Area provides operational connectivity services necessary to enable users access to information technology resources throughout the enterprise including those within the facility, between facilities, resources hosted at data centers, and connectivity to other systems. Network connectivity rules are enforced by VA approved baselines for router and switch configurations. The systems environment also includes as applicable, subsystem components such as tape drives, optical drives, disk drives, network area storage (NAS), storage access networks (SAN), archival appliances and tier 2 storage solutions. The systems boundary encompasses the management, operational, and technical security controls associated with IT hardware, consisting of servers, routers, switches, hubs, gateways, peripheral devices, desktop/laptops, and OS software. The Information Systems employ a myriad of routers and switches that connect to the VA network. The Area Boundary utilizes the VA Enterprise Cloud (VAEC).

Overview

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

- *The IT Area Boundary name and the name of the sites within it.*
- *The business purpose of the Area Boundary and how it relates to the program office and agency mission.*

- *Whether the Area Boundary is leveraging or accessing Enterprise repositories such as Veterans Benefits Management System, SharePoint, VistA, etc. and if so, a description of what PII/PHI from the Enterprise repositories is being used by the facilities in the Area Boundary.*
- *Documentation of any repository not maintained at the enterprise level, unlike Veterans Benefits Management System, SharePoint, VistA, etc. used by the facilities to collect, use, disseminate, maintain, or create PII/PHI.*
- *Any external information sharing conducted by the facilities within the Area Boundary.*
- *A citation of the legal authority to operate the Area Boundary.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *Does the Area Boundary host or maintain cloud technology? If so, Does the Area Boundary have a FedRAMP provisional or agency authorization?*

The White River Junction VA Medical Center (WRJ VAMC) VHA General Support System (GSS) is a facility level system that operates under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, §7301(a). GSS includes servers, workstations, laptops, printers and commercial-off-the-shelf applications) [Review applicable legal authorities and list all that apply to this system. Remember that all legal authorities listed here must also be consistent with legal authorities listed throughout this document]. It supports mission-critical and other systems necessary to conduct day-to-day operations by providing access to electronic resources.
The system contains and transmits contact, personal health, military, and financial information on veterans, their dependents, volunteers, employees, and contractors. The GSS is a new system that was created mid-year 2013, when the Office of Information and Technology made major changes to VA systems and their security boundaries. Consequently, Personally Identifiable Information (PII) and Sensitive Personal Information (SPI) now reside on this GSS. This data ownership remains at the facility level and many of the decisions related to the collection, use, storage, and dissemination of the data are

made at the facility level. [List the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual. Also list any hospitals/medical centers/regional offices that fall under this system.]
The VA White River Junction VA Medical Center (WRJ VAMC) GSS is an interconnected information resource under the same direct management control that shares common functionality. It includes local area network hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. The GSS is continuously used during business and non-business hours, supporting business processes related to the VA and its computing environment. The confidentiality, integrity and availability of the GSS is critical, i.e., ensuring that data is only received by the persons and applications that it is indented for, that data is not subject to unauthorized or accidental alterations, and that the resources are available when needed. Due to the sensitivity of the interconnected information resources of the GSS, all VA personnel with network/system access are required to have some type of a background investigation to fulfill their duties.
Internal sharing, discussed in greater detail in Section 4 of this Privacy Impact Assessment (PIA), is generally done to ensure that veterans and their families receive the benefits and care that they have earned. White River Junction VA Medical Center shares patient data with Vet Centers in addition to VA Central Office Cancer Registry, VA Network Authorization Office, VA Veterans Benefits Administration, VA Health Eligibility Center VA National Cemetery Administration, North East Consolidated Patient Account Center, and Consolidated Mail Outpatient Pharmacy . External sharing is discussed in greater detail in Section 5 of this PIA.

The applicable SORs for White River Jct. include:

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	***Applicable SORs***
VHA	• Accreditation Records-VA, VA SORN 01VA022 (May 18, 2009) • Applicants for Employment under Title 38, USC-VA, VA SORN 02VA135 (approved prior to 1995) • Blood Donor Information-VA, VA SORN 04VA115 (Dec. 12, 2008) • Individual Correspondence Records-VA, VA SORN 05VA026 (Nov. 26, 2008) • Employee Medical File System Records (Title 38)-VA, VA SORN 08VA05 • Employee Unfair Labor Practice Charges and Complaints, Negotiated Agreement Grievances and Arbitrations VA, VA SORN 09VA05 (approved prior to 1995) • Criminal Investigations-VA, VA SORN 11VA51 (Aug. 8, 2011) • Individuals Submitting Invoices-Vouchers For Payment-VA, VA SORN 13VA047 (approved prior to 1995) • Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attendings, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records-VA, VA SORN 14VA05135 (Nov.18, 2010) • Litigation Files-VA, VA SORN 16VA026 (March 16, 2009)

Site Type: VBA/VHA/NCA or Program Office	*Applicable SORs*
	• Centralized Staffing Systems-VA, VA SORN 18VA05 (approved prior to 1995) • Motor Vehicle Operator Accident Records-VA, VA SORN 20VA138 (Oct. 19, 2009) • Non-VA Fee Basis Records-VA, VA SORN 23VA16 (Aug. 31, 2009) • Patient Medical Records-VA, VA SORN 24VA10P2 (March 22, 2013) • Personnel and Accounting Integrated Data System-VA, VA SORN 27VA047 (July 02, 2012) • Personnel Registration under Controlled Substances Act-VA, VA SORN 28VA119 (Oct. 19, 2009) • Veterans, Employee and Citizen Health Care Facility Investigation Records-VA, VA SORN 32VA10Q (Aug. 31, 2009) • National Prosthetic Patient Database (NPPD)-VA, VA SORN 33VA113 (Oct. 19, 2009) • Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA, VA SORN 34VA12 (May 27, 2010) • VA Supervised Fiduciary/Beneficiary and General Investigative Records-VA, VA SORN 37VA27 (March 15, 2011) • Veterans and Beneficiaries Identification Records Location Subsystem-VA, VA SORN 38VA21 (June 4, 2001) • Veterans, Service Members, Family Members, and VA Beneficiary Survey Records-VA, VA SORN 43VA008 (April 06, 2007) • Health Administration Center Civilian Health and Medical Program Records-VA, VA SORN 54VA16 (July 15, 2009) • Voluntary Service Records-VA, VA SORN 57VA135 (April 15, 2009) • Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, VA SORN 58VA21/22/28 (July 19, 2012) • Repatriated American Prisoners of War-VA, VA SORN 60VA21 (Oct. 06, 2010) • Grievance Records-VA, VA SORN 63VA05 (approved prior to 1995) • Readjustment Counseling Program (RCS) Vet Center Program-VA, VA SORN 64VA15 (June 18, 2009) • Community Placement Program-VA, VA SORN 65VA122 (July 9, 2009) • PROS/KEYS, VA SORN 67VA30 (April 07, 2011) • VA Employee Counseling Services Program Records-VA, VA SORN 68VA05 (approved prior to 1995) • Ionizing Radiation Registry-VA, VA SORN 69VA131 (Dec. 08, 2008) • Health Professional Scholarship-VA, VA SORN 73VA10A2 (May 10, 2013) • General Personnel Records (Title 38)-VA, VA SORN 76VA05 (July 20, 2000) • Health Care Provider Credentialing and Privileging Records-VA, VA SORN 77VA10Q (March 26, 2008)

Site Type: VBA/VHA/NCA or Program Office	*Applicable SORs*
	• VA Police Badge and Training Records System-VA, VA SORN 83VA07 (Dec. 08, 2008) • National Chaplain Management Information System (NCMIS)-VA, VA SORN 84VA111 (May 08, 2009) • Chief Financial Officer and Fiscal Officer Designation and Certification Records System-VA, VA SORN 85VA047 (April 09, 2009) • Workers' Compensation Occupational Safety and Health Management Information System –VA, VA SORN 86VA00S1 (Aug. 05, 2008) • Customer User Provisioning System (CUPS)-VA, VA SORN 87VA005OP (Aug. 14, 2009) • Accounts Receivable Records (Formally known as 88VA20A6)-VA, VA SORN 88VA244 (Formally known as 88VA20A6) (April 6, 1998) • Income Verification Records-VA, VA SORN 89VA16 (May 08, 2008) • Call Detail Records-VA, VA SORN 90VA194 (April 14, 2009) • Electronic Document Management System (EDMS)-VA, VA SORN 92VA045 (May 2, 2000) • Gulf War Registry-VA, VA SORN 93VA131 (March 16, 2009) • Consolidated Data Information System-VA , VA SORN 97VA105 (May 04, 2011) • Disaster Emergency Medical Personnel System (DEMPS)-VA, VA SORM 98VA104 (Jan. 27, 2010) • Automated Safety Incident Surveillance and Tracking System-VA, VA SORN 99VA13 (March 31, 2009) • Patient Advocate Tracking System (PATS)-VA, VA SORN 100VA10NS10 (June 03, 3009) • Professional Standards Board Action and Proficiency Rating Folder (Title 38)-VA, VA SORN 101VA05 (July 20, 2000) • Agency-Initiated Personnel Actions (Title 38)-VA, VA SORN 102VA05 (July 28, 2000) • Police and Security Records-VA, VA SORN 103VA07B (Dec. 08, 2008) • Agent Orange Registry-VA, VA SORN 105VA131 (March 16, 2009) • Compliance Records, Response, and Resolution of Reports of Persons Allegedly Involved in Compliance • Violations-VA, VA SORN 106VA17 (Aug. 17, 2009) • Program Evaluation Research Data Records-VA, VA SORN 107VA008B (March 21, 2007) • Employee Incentive Scholarship Program-VA, VA SORN 110VA10 (Jan. 25, 2010) • Center for Acquisition and Material Management Education Online (CAMEO)-VA, VA SORN 111VA95E (Aug. 16, 2001)

Site Type: VBA/VHA/NCA or Program Office	*Applicable SORs*
	• Telephone Service for Clinical Care Records-VA, VA SORN 113VA112 (May 08, 2009) • The Revenue Program Billings and Collection Records-VA, VA SORN 114VA16 (Dec. 10, 2009) • Historical Alternative Dispute Resolution Data-VA, VA SORN 116VA08 (Feb. 02, 2012) • Veterans Canteen Service (VCS) Payroll Deduction System-VA, VA SORN 117VA103 (May 12, 2010) • Freedom of Information Act (FOIA) Records-VA, VA SORN 119VA005R1C (Nov. 17, 2009) • National Patient Databases-VA, VA SORN 121VA19 (May 11, 2012) • Center for Veterans Enterprise-VA, VA SORN 123VA00VE (Feb. 21, 2008) • My HealtheVET Administrative Records-VA, VA SORN 130VA19 (Nov. 17, 2010) • Purchase Credit Card Program-VA, VA SORN 131VA047 (March 31, 2009) • Library Network (VALNET)-VA, VA SORN 136VA19E (June 24, 2008) • Veterans Information Solutions (VIS)-VA, VA SORN 137VA005Q (July 28, 2009) • Veterans Affairs/Department of Defense Identity Repository (VADIR)-VA, VA SORN 138VA005Q (July 27, 2009) • Community Residential Care and Medical Foster Home Programs – VA, VA SORN 142VA114 (Nov. 01, 2011) • Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA , VA SORN 145VA005Q3 (March 25, 2008) • Department of Veterans Affairs Identity Management System (VAIDMS)-VA, VA SORN 146VA005Q3 (March26, 2008) • Enrollment and Eligibility Records-VA, VA SORN 147VA16 (Aug. 31, 2009) • Non-Health Data Analysis and Projections for VA Policy and Planning-VA, VA SORN 149VA008A (April 13, 2007) • Administrative Data Repository-VA, VA SORN 150VA19 (Nov. 26, 2011) • Inquiry Routing & Information System (IRIS)–VA, VA SORN 151VA005N (March 12, 2008) • Ethics Consultation Web-based Database (ECWeb)-VA, VA SORN 152VA10E (July 20, 2011) • Customer Relationship Management System (CRMS)-VA, VA SORN 155VA16 (Nov. 26, 2008) • Suicide Prevention Database-VA, VA SORN 158VA11 (Oct. 21, 2010) • Veterans Tracking Application (VTA)/Federal Case Management Tool (FCMT)-VA, VA SORN 163VA005Q3 (April 19, 2012) • Virtual Lifetime Electronic Record (VLER)-VA, VA SORN 168VA10P2 May 11, 2012)

Site Type: VBA/VHA/NCA or Program Office	*Applicable SORs*
VBA	• Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28

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, Area Boundary, or technology being developed.

1.1 What information is collected, used, disseminated, or created, by the facilities within the Area Boundary?

Identify and list all PII/PHI that is collected and stored in the Area Boundary, including 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. If the Area Boundary creates information (for example, a score, analysis, or report), list the information the Area Boundary is responsible for creating.

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

Please check any information listed below that the facilities within the area boundary collects. If additional PII/PHI is collected, please list those in the text box below:

☒ Name
☒ Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Account Information
☒ Health Insurance Beneficiary Numbers Account numbers
☒ Certificate/License numbers
☒ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Current Medications
☒ Previous Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☐ Other Unique Identifying Number (list below)

<<Add Additional Information Collected but Not Listed Above Here (For Example, A Personal Phone Number That Is Used as A Business Number)>>

PII Mapping of Components

White River Jct. consists of 5 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected within White River Jct. and the reasons for the collection of the PII are in the **Mapping of Components Table in Appendix B of this PIA.**

1.2 What are the sources of the information for the facilities within the Area Boundary?

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

Describe why information from sources other than the individual is required. For example, if a facility program within the Area Boundary is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the facility is using this source of data.
If a facility program within the Area Boundary creates information (for example, a score, analysis, or report), list the facility as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The information collected, maintained and/or disseminated by the WRJ system, inclusive of information collected in the VistA and District 1 GSS systems, is derived from various sources. The information may come directly from the Veteran or other programs and resources in the Veterans Benefits Administration (VBA), VA Health Eligibility Center (HEC), Department of Defense (DOD), VA Network Authorization Office (NAO) for non-VA care payments, and non-VA providers. Criminal background information is obtained from National Crime Information Center (NCIC) and used to confirm employment and/or volunteer eligibility and to assist the VA Police Service in conducting internal investigations. The information that resides on the (GSS) or is collected or maintained and/or disseminated by the White River Junction (GSS) VHA comes from a variety of sources. The largest amount of data comes directly from individuals - including veterans and their dependents, volunteers and other members of the public, clinical trainees, and VA employees and contractors. For example: items such as names, social security numbers, dates of birth are collected from the individual on healthcare enrollment forms (VA Form 10-10EZ), or other paperwork the individual prepares. An application for employment contains the same, or similar, information about employees. Depending on the type of information, it may also come from programs and resources in the Veterans Benefits Administration (VBA), the VA Health Eligibility Center (HEC), VA Network Authorization Office (NAO) for non-VA Care payments, and non-VA medical providers. In the case of a Veteran with a disability directly connected to their military service, the VBA may also provide service-connected disability ratings and information related to applicable disabilities (date granted, type of disability, overall percentage of combined
disabilities). Criminal background information is obtained from Electronic Questionnaires for Investigations Processing (E-QIP) and National Crime Information Center (NCIC) and used to confirm employment and/or volunteer eligibility and to assist the VA Police Service while conducting internal investigations.

Additional sources include:

- VA, Compensation, Pension, Education and Rehabilitation Records

- VA, Veterans and Beneficiaries Identification Records Location Subsystem
- VA, 36VA00 Veterans and Armed Forces Personnel United States Government Life Insurance Records
- VA, 46VA00 Veterans, Beneficiaries and Attorneys United States Government Insurance Award Records
- VA, Veterans and Beneficiaries Identification and Records Location (BIRLS)
- Compensation, Pension, Education and Rehabilitation (covers BDN and Corporate databases)
- Loan Guaranty Home, Condominium and Manufactured Home Loan Applicant Records
- VA. 53VA00 Veterans Mortgage Life Insurance

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information collected from individuals is collected verbally in interview 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 done using hard copy format via fax, secure web portals and VPN connections as well as facility identified resources.
Information collected directly from patients, employees and/or other members of the public is collected using paper forms (such as the VA Form 10-10EZ enrollment form for VA health care), or interviews and assessments with the individual. Information related to an employee's employment application may be gathered from the applicant for employment, which is provided to an application processing website, USA Jobs located at https://www.usajobs.gov/. Much of the information provided by veterans or other members of the public, such as address and phone number, next of kin and emergency contact information, and similar information are assumed to be accurate because it is provided directly by the individual.
Additionally, information entered into an individual's medical record by a doctor or other medical staff is also assumed to be accurate.
Information from outside resources comes to VA White River Junction GSS using several methods. Chief among these sources, are the DoD, VBA, SSA, and IRS. The DoD provides military records, including medical records compiled when the patient was a member of the US Military. The VBA provides records which include the type and percentage of granted 'service-connected' disabilities, the dates of service-connected disability ratings, and, in some cases, the VBA populates patient to provide a Compensation and Pension examination to a claimant. Income information is verified using information from the Social Security Administration (SSA) and the Internal Revenue Service (IRS).
These data collections may be done using secure web portals, VPN connection, e-mail, facsimile, verbally and/or using paper files.

Means of Collection Table

Site Type: VBA/VHA/NCA or Program Office	***Means of Collection***
VHA	Information collected directly from patients, employees and/or other members of the public is collected using paper forms (such as the VA Form 10-10EZ enrollment form for VA health care), or

Site Type: VBA/VHA/NCA or Program Office	*Means of Collection*
	interviews and assessments with the individual. Much of the information provided by veterans or other members of the public, such as address and phone number, next of kin and emergency contact information, and similar information are assumed to be accurate because it is provided directly by the individual. Additionally, information entered into an individual's medical record by a doctor or other medical staff is also assumed to be accurate.
VBA	There are many VA forms used by Veterans to apply for and/or make adjustments to pending benefits. All VBA benefit forms are located at http://www.va.gov/vaforms/. The URL of the associated privacy statement is: http://www.va.gov/privacy/. VBA forms can be downloaded from this site, filled in and printed to be delivered in paper form. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury. The VBA toll free number for veterans is 1-800-827-1000. Clients are referred to and transferred to the Regional Office of Jurisdiction, where they can provide a service representative with required information. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury. VBA employees may also contact a Veteran directly to obtain clarifying information for a claim for benefits.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular PII/PHI is collected, maintained, used, or disseminated in the Area Boundary is necessary to the program's or agency's mission. Merely stating the general purpose of the Area Boundary without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the Area Boundary collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the Area Boundary's purpose.
This question is related to privacy control AP-2, Purpose Specification.

The purposes of the information from Veterans and other members of the public collected, maintained, and processed by the VA White River Junction GSS are as varied as the types of information collected. Much of the information collected is maintained, used, and disseminated to ensure that Veterans and other eligible individuals obtain the medical and mental health treatment they require. Additional information, such as bank account information and insurance information are used to process claims and requests for benefits. Other purposes include determination of legal authority for providers and other clinical staff to practice medicine and/or subject matter expertise, release of information request responses, and research/analysis of data.

1. Determine eligibility for health care and continuity of care
2. Emergency contact information
3. Provide medical care
4. Communicate with Veterans/Patients and their families or emergency contacts
5. Determine legal authority for providers and health care workers to practice medicine
6. Respond to Release of Information requests
7. Third Party health insurance billing
8. Contact for employment eligibility and verification

Purpose of Information Collection Table

Site Type: VBA/VHA/NCA or Program Office	***Purpose of Information Collection***
VHA	• To determine eligibility for health care and continuity of care • Emergency contact information is cases of emergency situations such as medical emergencies • Provide medical care • Communication with Veterans/patients and their families/emergency contacts • Determine legal authority for providers and health care workers to practice medicine and/or subject matter expertise • Responding to release of information request • Third party health care plan billing, e.g. private insurance • Statistical analysis of patient treatment • Contact for employment eligibility/verification
VBA	• Compensation and Pension • Education • Vocational Rehabilitation and Employment • Loan Guaranty • Insurance • The primary services of the benefit systems entail the receipt, processing, tracking and disposition of Veterans' application for benefits and requests for assistance, and the general administration of legislated benefit programs. Information is collected to provide all entitled benefits in the most complete and effective manner.

1.5 How will the information collected and used by the facilities be checked for accuracy? How often will it be checked?

Discuss whether and how often information stored in a facility within the Area Boundary is checked for accuracy. Is information within the facility 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 a facility within the Area Boundaries that receives data from internal data sources or VA IT systems, describe the checks to ensure that data corruption has not occurred during transmission.

If the Area Boundary checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Information obtained directly from the individual will be assumed to be accurate. Furthermore, individuals have the right to obtain access to their records and request correction to them when necessary (see Section 7 for additional information). Patient demographic information as well as income verification matching information is completed by automated tools with connections to the Austin Automation Center. Practitioners review and sign all treatment information.
Various staff review data obtained and Health Information Management staff assist with corrections. Data is matched against supporting documentation submitted by the Veteran, i.e., social security card, DD- 214, drivers license, military ID. Social Security Numbers are also verified through the Social Security Administration (SSA) to determine financial eligibility. VBA is used to verify eligibility for VA benefits. The VA verifies military service information through DOD. Financial information is verified through the SSA and Internal Revenue Service (IRS).
Employee, contractor, students and volunteer information is obtained by automated tools as well as obtained directly by the individuals. The Office of Personnel Management is contacted to obtain background reviews. Provider credentialing information is obtained from a variety of education resources and clinical privileging services.

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

List the full legal authority for operating the Area Boundary, 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

WRJ GSS system operates under the following legal authorities.

Legal Authority Table

Site Type: VBA/VHA/NCA or Program Office	Legal Authority
VHA	• **Veterans Benefits**, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b) • **Veteran's Health Administration – Organization and Functions**, Title 38, U.S.C., Chapter 73, § 7301(a) • Health Insurance Portability and Accountability Act of 1996 (HIPAA) • Health Information Technology for Economic and Clinical Health (HITECH) Act • Privacy Act of 1974 • Freedom of Information Act (FOIA) 5 USC 552 • VHA Directive 1605.01 Privacy & Release of Information • VA Directive 6500 Managing Information Security Risk: VA Information Security Program.
VBA	• Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b)

Site Type: VBA/VHA/NCA or Program Office	Legal Authority
VHA	• **Veterans Benefits**, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b) • **Veteran's Health Administration – Organization and Functions**, Title 38, U.S.C., Chapter 73, § 7301(a) • Health Insurance Portability and Accountability Act of 1996 (HIPAA) • Health Information Technology for Economic and Clinical Health (HITECH) Act • Privacy Act of 1974 • Freedom of Information Act (FOIA) 5 USC 552 • VHA Directive 1605.01 Privacy & Release of Information • VA Directive 6500 Managing Information Security Risk: VA Information Security Program.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Privacy Risk:

WRJ 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 date were accessed by an unauthorized individual or if the data was otherwise breached, serious harm or even identity theft may result.

Mitigation:

WRJ deploys extensive security measures to protect the information from inappropriate use and/or disclosure. This is done by means of both access controls and training of all employees and contractors. WRJ 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, program management, and planning and maintenance. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization, individual participation and redress, transparency, and use limitation.

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 within the Area Boundary 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 use of information for day-to-day business needs applies to the WRJ system, inclusive of information collected in the District 1 GSS systems. 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, vehicle license plate number, 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.

- **Name**: Used to identify the patient during appointments and in other forms of communication
- **Social Security Number**: Used as a patient identifier and as a resource for verifying income Information with the Social Security Administration
- **Date of Birth**: Used to identify age and confirm patient identity
- **Mother's Maiden Name:** Used to confirm patient identity
- **Mailing Address**: Used for communication, billing purposes and calculate travel pay
- **Zip Code**: Used for communication, billing purposes, and to calculate travel pay
- **Phone Number(s):** Used for communication, confirmation of appointments and conduct Telehealth appointments
- **Fax Number**: used to send forms of communication and records to business contacts, Insurance companies and health care providers
- **Email Address**: used for communication and MyHealtheVet secure communications
- **Emergency Contact Information (Name, Phone Number, etc. of a different individual):** Used in cases of emergent situations such as medical emergencies.
- **Financial Account Information:** Used to calculate co-payments and VA health care benefit eligibility
- **Health Insurance Beneficiary Account Numbers**: Used to communicate and bill third part Health care plans
- **Certificate/License numbers**: Used to track and verify legal authority to practice medicine and Licensure for health care workers in an area of expertise.

- **Internet Protocol (IP) Address Numbers**: Used for configuration and network connections. Network Communication allows information to be transferred from one Information Technology System to another.
- **Current Medications**: Used within the medical records for health care purposes/treatment, prescribing medications and allergy interactions.
- **Previous Medical Records**: Used for continuity of health care
- **Race/Ethnicity**: Used for patient demographic information and for indicators of ethnicity-related diseases.
- **Next of Kin**: Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
- **Guardian Information**: Used when patient is unable to make decisions for themselves.
- **Electronic Protected Health Information (ePHI):** Used for history of health care treatment, during treatment and plan of treatment when necessary.
- **Military history/service connection**: Used to evaluate medical conditions that could be related to location of military time served. It is also used to determine VA benefit and health care eligibility.
- **Service connected disabilities**: Used to determine VA health care eligibility and treatment plans/programs
- **Employment information**: Used to determine VA employment eligibility and for veteran contact, financial verification.
- **Veteran dependent information**: Used to determine benefit support and as an emergency contact person.
- **Disclosure requestor information**: Used to track and account for patient medical records released to requestors.
- **Death certificate information**: Used to determine date, location and cause of death.
- **Criminal background information**: Used to determine employment eligibility and during VA Police investigations.
- **Education Information**: Used for demographic background information for patients and as a determining factor for VA employment in areas of expertise. Basic educational background, e.g. High School Diploma, college degree credentials
- **Gender**: Used as patient demographic, identity and indicator for type of medical care/provider and medical tests required for individual.
- **Tumor PII/PHI Statistics**: Used to evaluate medical conditions and determine treatment plan

The data may be used for approved 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; the registration of vehicles and the assignment and utilization of parking spaces; 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.

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

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

If the facility creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

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

The VA White River Junction GSS system uses statistics and analysis to create general reports that provide the VA a better understanding of patient care and needs. These 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. Analyze appointment time-frame data to track and trend averages of time.
4. Other tools are:
    a. AbbottLink Alere RALS-Plus
    b. Bar Code Medication Administration Carestream PACS
    c. CPRS
    d. DSS/Quadramed Encoder Product Suite/VIP DSS Dental Records Manager Plus (DRM Plus) DSS Fee Basis Claims Suite
    e. DSS Mental Health Suite Holter System
    f. Merge Eye Care PACS
    g.

h. Mumps AudioFAX MUSE/EKG System Omnicell
i. Philips Healthcare RAI/MDS
j. Scripto
k. Sysmex America Telerecord Manager Topcon Medical Imaging Vecna VetLink
l. VistA RAD

These reports may track:

- The number of patients enrolled, provider capacity, staffing ratio, new primary care patient wait time, etc. for Veterans established with a Patient Care Aligned Team (PACT)
- Beneficiary travel summary/benefits
- Workload and cost resources for various services, i.e., mental health, primary care, home dialysis, fee services, etc.
- Daily bed management activity
- Coding averages for outpatient/inpatient encounters
- Satisfaction of Healthcare Experience of Patients (SHEP) data as it pertains to customer satisfaction regarding outpatient/inpatient services
- Unique patient trends
- Clinic wait times
- Letters to veterans concerning the progress of their claim are generated periodically, as well as rating decisions and requests for additional information to substantiate the claim. These letters are generated electronically and printed on paper and mailed to the veteran.

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

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 Area Boundary 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 facilities 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.

The controls in place to assure the information is handled in accordance with the uses described above include mandatory online information security and HIPAA training; face-to-face training for all incoming employees conducted by the Information Security Officer and Privacy Officer; regular audits of accessions of sensitive information; and formal rounds during which there is personal examination of all areas within the facility to ensure information is being appropriately used and controlled. Disciplinary policies are in place to address unauthorized and unapproved use of data and include the most appropriate of the following: re-training, re-education, removal of access privileges, counselling, admonishment, reprimand, suspension and removal.

Privacy Risk

The controls in place to assure that the information is handled in accordance with the uses described above include mandatory online information security and HIPAA training; face-to-face training for all incoming employees conducted by the Information Security Officer and Privacy Officer; regular audits of individuals accessing sensitive

information; and formal rounds during which personal examination of all areas within the facility to ensure information is being appropriately used and controlled.
System sign-on banners are displayed prior to system sign-on, which notify the user that the VA system is intended to be used by authorized users for official government business and misuse of the system is prohibited.

Mitigation:
Additionally, after a thorough fact-finding, those found in violation of HIPAA, Privacy Act, Privacy or Security Rule, or local privacy and/or Information Security policies are required to complete additional training depending on the severity of the offense. Specific training developed and presented by local Privacy Office to address refresher needs, as identified by fact-findings, to date includes: Entering Employee Medical Records Improving Auditory Privacy, and Careful What You Disclose. Office of Human Resource Management's Table of Penalties is also utilized by the Associate Director when determining if administrative action is warranted.

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 by the facilities within the Area Boundary?

Identify and list all information collected from question 1.1 that is retained by the facilities within the Area Boundary.

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

The following applies to the WRJ system and is inclusive of information collected in the VistA and District 1 GSS systems. Information retained is based on national VA policies. Below is a list of information that may be retained.

- Name
- Previous medical records
- Social Security Number (SSN)
- Race/ethnicity
- Date of Birth
- Next of Kin
- Mother's Maiden Name
- Guardian Information
- Mailing Address
- ePHI
- Zip Code
- Military history/service connection
- Phone Numbers
- Service connection disabilities
- Fax Numbers
- Employment information
- Email address
- Veteran dependent information
- Emergency contact info
- Disclosure requestor information
- Financial account information
- Death certification information
- Health insurance beneficiary account numbers

- Tumor PII/PHI statistics
- Certificate/license numbers
- Criminal background investigation
- Internet Protocol address numbers
- Education Information
- Current medications
- Gender

3.2 How long is information retained by the facilities?

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 Area Boundary may have a different retention period than medical records or education records held within your Area Boundary, 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.

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

These documents specify 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 at the Veteran's Health Administration, please review RCS 10-1 and RCS 005-1 at the above links. Below are some key record retention schedules for the WRJ system, inclusive of information collected in the VistA and District 1 GSS systems.

Length of Retention Table

Site Type: VBA/VHA/NCA or Program Office	***Length of Retention***
VHA	• 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, Part Two, Chapter Four- Finance Management • 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, Part Three, Chapter Six- Healthcare Records, Item 6000.1a. and 6000.1d. • 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, Part Two, Chapter Three- Civilian Personnel, Item No. 3000.1 • Office of Information & Technology (OI&T) Records: These records are created, maintained and disposed of in accordance with Department of Veterans Affairs, Office of Information & Technology RCS 005-1.
VBA	• Compensation, pension, and vocational rehabilitation claims folders are retained at the servicing regional office until they are inactive for three years, after which they are transferred to

Site Type: VBA/VHA/NCA or Program Office	*Length of Retention*
	the Records Management Center (RMC) for the life of the Veteran. • Official legal documents (e.g., birth certificates, marriage licenses) are returned to the claimant after copies are made for the claimant's file. At the death of the Veteran, these records are sent to the Federal Records Center (FRC) and maintained by the National Archives and Records Administration (NARA) in accordance with NARA policy. • Once a file is electronically imaged and accepted by VBA, its paper contents (with the exception of documents that are the official property of the Department of Defense, and official legal documents), are destroyed in accordance with Records Control Schedule VB–1 Part 1 Section XIII, as authorized by NARA. • Documents that are the property of the Department of Defense are either stored at the RMC or transferred to NARA and maintained in accordance with NARA policy. • Vocational Rehabilitation counseling records are maintained until the exhaustion of a Veteran's maximum entitlement or upon the exceeding of a Veteran's delimiting date of eligibility (generally, ten or twelve years from discharge or release from active duty), whichever occurs first, and then destroyed. • Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA. • Education electronic folders are retained at the servicing Regional Processing Office. Education folders may be destroyed in accordance with the times set forth in the Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA. • Employee productivity records are maintained for two years after which they are destroyed by shredding.

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the Area Boundary owner.
This question is related to privacy control DM-2, Data Retention and Disposal.
When managing and maintaining VA data and records, WRJ, inclusive of information collected in the VistA and District 1 GSS systems, follows the guidelines established in the NARA-approved schedules listed in the table below.

Site Type: VBA/VHA/NCA or Program Office	***Retention Schedule***
VHA	Records Control Schedule 10-1 Records Control Schedule 005-1
VBA	Veterans Benefits-1

3.4 What are the procedures for the elimination of PII/PHI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.?

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

Information within the White River Junction VA Medical Center GSS is destroyed by the disposition guidance of RCS 10-1.
Once the information retention period is reached, Record Management and Office of Information Technology will develop a plan for disposal or deletion. The plan will be routed for approval and implementations through VA and the National Archives, and will be derived from the following existing guidance:
Paper documents are destroyed to an unreadable state in accordance with the Department of Veteran's Affairs VA Directive 6371, (April8, 2014). http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2.
Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records and more are destroyed in accordance with the Department of Veteran's Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=416&FType=2. When required, this data is deleted from the file location and then permanently deleted from the deleted items location or recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per Handbook 6500.1.
Additionally, the White River Junction VHA White River Junction follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents **as well as** FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.
Hard copy documents that qualify as official records are handled in accordance with the record control schedules listed previously. Any temporary records or those authorized for disposal by the appropriate control schedule are stored in secure containers until contracted personnel can collect them and shred the documents inside in accordance with VA Directive 6371 Destruction of Temporary Paper Records. The contractors provide a certificate of destruction to Facility Management Service. The paper waste is collected and sent off for pulping. Any contractors performing the on-site shredding services are certified through the National Association for Information Destruction (NAID).
Information stored electronically will be disposed of in accordance with VA Handbook 6500.1 Electronic Media Sanitization. Information is removed from media using VA approved methods prior to storage devices leaving VA control. When this is not possible the devices are rendered unreadable. Once information is removed from media or media is rendered unreadable the media is sent via registered courier to a destruction facility where the media is destroyed in such a manner that information can no longer be recovered from it. A chain of custody is maintained through the destruction process and a certificate of destruction is maintained by the VA and destruction facility.
Paper records are shredded on-site by a shredding company, witnessed by the Records Management Officer, and are accompanied by a certificate of destruction. Non-paper records maintained on magnetic media are

destroyed by erasing the magnetic media using an approved software to digitally overwrite the media. The media is then shredded on-site by the contracted shredding company, witnessed by the Records Management Officer per VBA Directive 6300.

3.5 Does the Area Boundary include any facility or program that, where feasible, uses techniques to minimize the risk to privacy by using PII for research, testing, or training?
Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

All research protocols are reviewed by the Privacy Officer and the Information Security Officer to make sure that all data is protected wherever it resides.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Privacy Risk:
There is a risk that the information 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 in the WRJ system is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary. The Records Manager ensures data retention policies and procedures are followed. The Privacy Officer, Information Security Officer, and Chief Information Officer monitor controls to mitigate any breaches of security and privacy.

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 are facilities within the Area Boundary sharing/receiving/transmitting information with? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Note: Question #3.6 (second table) in the Area 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 Area Boundary 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 each facility, 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.

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Department of Veterans Affairs Office of Inspector General (OIG)	Litigations or potential litigations. Consultations. Assistance in investigation of patient or employee claims.	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) appropriate to the request.	Transmitted upon request in an electronic, verbal, or written format based on the individual request.
VA Central Office Cancer Registry	Tracking and trending of diseases	Diagnosis, tumor status, treatment outcome, survivor tracking, type of treatments, demographics, hormone radiation, chemotherapy and problem lists	Oncotrax
VA Network Authorization Office: Non-VA Care Payments	Health/Medical Payment Authorization	Demographics, diagnosis, medical history, service connection, provider orders, VHA recommendation/approval for Non-VA care	Fee Basis Claim System (FBCS) software program
VA Veterans Benefits Administration	Service-connected/non-service connected disabilities, benefits payments, educational benefits, spousal benefits	Financial Assessment Test and service-connected disability diagnosis, veterans' health status, compensation and pension exam notes	Compensation and Pension Record Interchange (CAPRI)
VA Health Eligibility Center (HEC)	Medical Care Cost Recovery	Diagnosis, service connection, dates of service, health insurance information, demographics	Enrollment Systems Redesign or automatic upload to HEC via a VistA entry
VA National Cemetery Administration	Death/burial benefits	Veteran's names, SSN, character of service, DD214	Secure fax
North East Consolidated Patient Account Center	Medical Care Cost Recovery	Diagnosis, service connection, dates of service, health insurance information, demographics	VistA
Consolidated Mail Outpatient Pharmacy (CMOP)	For a complete patient profile of controlled substances	Veteran's name, address, full SSN, DOB, provider's name, name/quantity of medication(s),	VistA
Vet Centers	Continuity of care, eligibility, enrollment	Read Only Access to health information for plan of treatments	Electronically reviewed through CPRS

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Privacy Risk: The sharing of data is necessary for the medical care of individuals eligible to receive care at VHA and District 1 facilities. 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, program management, planning and maintenance. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation.

The Electronic Computer Access Request (ECAR) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

The use of Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two0factor authentication.

Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

Microsoft Outlook is also another tool that is used to share internal information within the organization, Risks are mitigated by using encryption methods to share sensitive information within the organization.

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 facility is allowed to share the information in identifiable form or personally identifiable information outside of VA.

Note: Question #3.7 in the Area 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 an Area Boundary outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

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 data element types such as PII/PHI that are shared/received 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***
New Hampshire Department of Health and Human Services	Tracking of infectious diseases	Health information regarding infectious disease, patient's name, lab results, and contact information	MA and VT state laws SORN 02VA135 Each State Specific law are in each Standing Letter	Via secure fax
Social Security Administration /Social Security Disability	Payment/Disability Benefits	Social Security Number, Protected Health Information (PHI)	Title 38, U.S.C. Section 5701 SORN 79VA19, SORN 02VA135	Via a secure link Electronic Records
Vermont Department of Health	Tracking of infectious diseases	Health information regarding infectious disease, patient's name, lab results, and contact information	MA and VT state laws SORN 02VA135 Each State Specific law are in each Standing Letter	Via secure fax
Office of Personnel Management	Assistance in employment and personal identity	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) appropriate to the agreement.	ISA/MOU; Title 38, United States Code, Section 5701, Section 511.202 of title 5, Code of Federal Regulations	Electronic, paper, verbal
Internal Revenue System	Information is shared as the IRS requires the use of identifying data, including names and social security numbers, in order for VA to request and receive unearned	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually	National ISA/ MOU	Secure Web-Portal, Secure Socket Layer, web connections are using FIPS 140-2 secure connections
Dept of Defense	Sharing data and other information resources used to deliver healthcare, benefits and administrative data	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) appropriate to the agreement.	ISA/ MOU for DoD, Privacy Act 1974, 5 USC 552a, HIPAA, NIST 800-47	Secure web portal, web connections are using FIPS 140-2 secure connections

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

Access controls, audit and accountability, awareness and training, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, media protection, personnel security, physical and environmental protection, risk assessments, system and services acquisition, system and communication protection, system and information integrity, planning and maintenance are used to meet the requirements of OMB Memoranda M-06-15 andM-06-16.

The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.

The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.

The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for Veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.

Internal protection is managed by access controls such as user authentication (user IDs, passwords and Personal Identification Verification (PIV)), awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

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

Follow the format below:

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

.

Mitigation: **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, program management, planning and maintenance.

Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

All personnel accessing Veteran's information must first have a successfully adjudicated background screening (SAC). This background check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history record. A background investigation is required commensurate with the individual's duties.

Individual users are only given job position specific access to individually identifying data through the issuance of a user ID and password. Memorandum of Understanding/Interconnectivity Service Agreements (MOU/ISA's), Business Associate Agreements (BAA's), contracts and other legal documents that authorize that sharing of data between the VA and an external entity are reviewed on a routine basis.

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 in Appendix A. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

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

This question is related to privacy control TR-1, Privacy Notice, and TR-2, Area Boundary of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A signed statement acknowledging that the individual read and understood NOPP is scanned into each applicant electronic file. When updates are made to the NOPP, copies are mailed 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 Department of Veterans Affairs provides additional notice of this system by publishing two System
of Record Notices (SORNs):

1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Feb. 11, 2014) in the Federal Register and online. An online copy of the SORN can be found at: http://www.gpo.gov/fdsys/pkg/FR-2014-02-11/pdf/2014-02890.pdf.

2) The VA System of Record Notice (VASORN) Veterans Health Information System and Technology Architecture (VISTA)-VA, SORN 79VA10P2 (Amended Oct. 31, 2012) in the Federal Register and online. An online copy of the SORN can be found at: http://www.gop.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26804.pdf.

This PIA also serves as notice of the WRJ system. 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." The following VA Systems of Record
Notices (SORNs) which are published in the Federal Register available online:

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	***Applicable SORs***
VHA	• Applicant for Employment under Title 38, USC-VA, SORN 02VA135 • Individuals serving on a Fee Basis or Without Compensation (Consultants, Attending's and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records-VA, SORN 14VA05135 (November 18, 2010) • Non-VA Fee Basis Records-VA SORN 23VA163 (August 31, 2014) • Patient Medical Records-VA, SORN 24VA19 (March 22, 2013) • Veteran, Patient, Employee and Volunteer Research and Development Project Records-VA, SORN 34VA12 (May 27, 2010) • Community Placement Program-VA, SORN 65VA122 • Health Care Provider Credentialing and Privileging Records-VA, SORN 77VA10Q (June 25, 2014) • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SORN 79VA10P2 (October 31, 2012, as amended) • Income Verification Records-VA, SORN 89VA19 (May 8, 2008) • Automated Safety Incident Surveillance and Tracking System-VA, SORN 99VA131 (March 31, 2009) • Telephone Service for Clinical Care Records-VA, SORN 113VA112 (May 8, 2009) • The Revenue Program Billings and Collections Records-VA, SORN 114VA16 (December 10, 2009 as amended) • National Patient Database-VA, SORN 121VA19 (May 11, 202 as amended)
VBA	• Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached.

This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

The Veterans' Health Administration (VHA) requests only information necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information to the VHA, this may prevent or delay them from obtaining the benefits necessary for them.

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with the VA. Individuals can decline to provide information without penalty except for the means test process. Non-service connected Veterans and Veterans who are in receipt of service-connected compensation of less than 50% may decline to give means test information but are informed the withholding of information may result in being placed in a category 8 which they are billed for certain services.

6.3 Do individuals have the right to consent to 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

Individuals have a right to deny the use of their health information and/or individually identifiable health information for the purpose of research.

Veterans may utilize the 10-5345 (Request for Authorization to Release Medical Records or Health Information) to state with whom his/her information may be shared.

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 restrict information is accepted the facility must conform to the restrictions.
Veterans have the right to opt out of the facility directory.

Information Consent Rights Table

Site Type: VBA/VHA/NCA or Program Office	***Information Consent Rights***
VHA	Yes. Individuals must submit in writing to their facility PO. The request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, no information on the individual is given out. Individuals can request further limitations on other disclosures. A veteran, legal guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information.
VBA	Once information is provided to VBA, the records are used, as necessary, to ensure the administration of statutory benefits to all eligible Veterans, Service members, reservists, and their spouses, surviving spouses and dependents. As such, individuals are not provided with the direct opportunity to consent to uses of information. However, if an individual wishes to remove consent for a particular use of their information, they should contact the nearest VA regional office, a list of which can be found on the VBA website.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

Follow the format below:

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

Mitigation: Mitigation: The risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPP's are mailed to beneficiaries on a yearly basis and periodic monitoring is performed to check that the signed acknowledgement 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 a 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?

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 to obtain information about FOIA points of contact and information about agency FOIA processes.

If the facilities within the Area Boundary are exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the facilities within the Area Boundary are not a Privacy Act Area Boundary, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

The following applies to the WRJ system, inclusive information collected in the VistA system. This section has no application within the District 1 GSS system.

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 a medical facility's Release of Information (ROI) office. Requests for public information may be forwarded to the facility's Freedom of Information Act Officer. When requesting access to one's own records, patients are asked to complete VA Form 10-5345a (Individuals' Request for a Copy of their Own Health Information) which can be obtained from the medical center or online at http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf.

Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information in the VistA system. Contractors should contact their Contract Officer Representative to correct inaccurate or erroneous information that may be required in the VistA system.

As directed in VA SOR Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28(July 19, 2012), individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. A list of regional VA offices may be found on the VBA Website.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

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**.

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that

even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.

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

The following applies to the WRJ system, inclusive of information collected in the VistA system. This section has no application within the District 1 GSS system.

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 area 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).

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

The following applies to the WRJ system, inclusive of information collected in the VistA system. The Privacy Officer provides appeal rights to the Office of General Council or VHA Privacy Office via the written response to the Veteran regarding the outcome of the amendment request.

Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3

In addition to the formal procedures discussed in question 7.2 to request changes to one's health record, a veteran or other VAMC patient who is enrolled in myHealth*e* vet can use the system to make direct edits to their health records.

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 Area Boundary and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

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

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

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

Privacy Risk: Privacy Risk: There is a risk that a Veteran may not know how to obtain access to their records or how to request corrections to their records and that the medical record could contain inaccurate information and subsequently effect the care the Veteran receives.

Mitigation:

- As discussed in question 7.3, the Notice of Privacy Practice (NOPP), which every patient must sign prior to receiving treatment, it discusses the process for requesting an amendment to ones' records. Beneficiaries are reminded of the information when the NOPP is mailed to them yearly.
- 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 the MyHealthE Vet program to provide Veterans remote access to their medical records. The Veteran must enroll to obtain access to all the available features.
- In addition, Privacy Handbook 1605.2 establishes procedures for Veterans to have their records amended where appropriate.

Additionally, the WRJ staff is informed of the importance of maintaining compliance with the VA Release of Information (ROI) policies and procedures and the importance of remaining alert to

information correction requests.

Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information in the VistA system. Contractors should contact their Contract Officer Representative to correct erroneous information that may be required in the VistA system.

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 Area Boundary, and are they documented?

Describe the process by which an individual receives access to the Area Boundary.

Identify users from other agencies who may have access to the Area Boundary and under what roles these individuals have access to the Area Boundary. Who establishes the criteria for what PII can be shared?

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

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

Individuals receive access to the WRJ system by gainful employment in the VA or upon being awarded a contract that requires access to the VistA system and/or District 1 GSS system. Individuals are given the minimal access to records to complete their duties. Upon hire, position change or job assignment change, the supervisor is to review the individual's access to the system and to protected health information to ensure the correct level of access is maintained. This review is also repeated annually and is documented on the VA Form 10-0539, *Assignment of Functional Categories.* If contracted individuals receive access to our system, their access would be requested and approved by the Service entering into the contract. They also would only be given access to the programs/information needed to complete their duties. Access is requested per DVA and WRJ policies utilizing Electronic Computer Access Requests (ECAR) and other individual local processes. Users submit access requests based on need to know and job duties. Multiple disciplinary levels must be obtained prior to access being granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval process. Once access is gained, individuals can log into the system(s) through dual authentication. i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need to know basis.
Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and they are protected from outside

Full time VARO employees, as their job requires it, have access to change Veteran Service Representative (VSR) and (RVSR) Rating Veteran Service Representatives have access to

amend/change the information in the system, under the guidelines of least privilege, that is, users are granted the minimum accesses necessity to perform their duties. Work Study's' are limited to Inquiry only commands. Veteran Service Organizations (Co-located VSOs) and County or Out based VSOs (CVSOs) also have access to VA systems. These accesses are predefined and limited for these users. Individuals are subject to a background investigation before given access to Veteran's information. Private Attorneys, Claim Agents and Veteran Service Organizations Representatives must be accredited through the Office of General Counsel.

8.2 Will VA contractors have access to the Area Boundary and the PII? If yes, what involvement will contractors have with the design and maintenance of the Area Boundary? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the Area Boundary?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the Area Boundary 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.

Contractors may have access to the WRJ system, inclusive of the VistA and GSS systems, on a need-to-know basis in the performance of their contracted assignments/tasks, 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 can have access to the system only after completing mandatory annual information security and privacy training as well as reading and agreeing to VA Contractor Rules of Behavior. VHA HIPAA Privacy Training as well as the appropriate background investigation to include fingerprinting is required. 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.

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

VA offers privacy and security training. Each program or Area Boundary may offer training specific to the program or Area Boundary 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 WRJ personnel, volunteers, and contractors are required to complete initial and annual Privacy and Security Awareness and Rule Behavior (RoB) training, during New Employee Orientation

(NEO) or via TMS. In addition, all employees who interact with patient sensitive medical information must complete the Privacy and HIPAA focused mandated privacy training. Finally, all new employees receive face-to-face training by the area Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officers also perform subject specific trainings on an as needed basis.

Each site identifies personnel with significant information system security roles and responsibilities. (i.e., management, system managers, system administrators, contracting staff, HR staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained. The Talent Management System offers the following applicable privacy courses:

VA 10176: Privacy and Information Security Awareness and Rules of Behavior
VA 10203: Privacy and HIPPA Training
VA 3812493: Annual Government Ethics.

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

If Yes, provide:

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

Please note that all Area Boundaries containing PII/PHI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

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

The most recent ATO's for the District 1 GSS and District 1 VistA were granted in August 2015. The WRJ system does not have an ATO date as it is assessed at the enterprise level. The "ATO Granted Date" is 5/24/2019.

The WRJ falls under District 1 and both systems are categorized as high risk under the Federal Information Processing Standards Publication 199. The WRJ system is continually monitored through the self-assessment of the controls assigned to the system in the GRC tools. The self-assessment is conducted by the Chief Information Officer and the information Security Officer and the assessment is reviewed at the national level.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced Area Boundary 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	Area Boundary of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

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

Signature of Privacy Officers

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

Digitally signed by JOSEPH A SMERALDI 3376862
Date: 2021.08.23 15:06:42 -04'00'

Area Privacy Officer, Joseph Smeraldi

Joseph D Friesenhahn 1563772

Digitally signed by Joseph D Friesenhahn 1563772
Date: 2021.08.23 15:10:26 -04'00'

Area Boundary Information System Security Officer, Joseph Friesenhahn

matthew d rafus 123679

Digitally signed by matthew d rafus 123679
Date: 2021.08.23 15:16:57 -04'00'

Area Boundary Manager, Matthew Rafus

APPENDIX A – Notice

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).

Applicable Notices

Site Type: VBA/VHA/NCA or Program Office	***Applicable NOPPs***
VHA	**Notice of Privacy Practices** **VHA Privacy and Release of Information:**
VBA	**Privacy Statement on VA Forms:** PRIVACY ACT INFORMATION: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA Programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is required to obtain or retain benefits. VA uses your SSN to identify your claim file. Providing your SSN will help ensure that your records are properly associated with your claim file. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by Federal Statute of law in effect prior to January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine maximum benefits under the law. The responses you submit are considered confidential (38 U.S.C. 5701). Information submitted is subject to verification through computer matching programs with other agencies **SOR 58VA21/22/28**

APPENDIX B – PII Mapped to Components

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

PII Mapped to Components Table

Components of the Area Boundary collecting/storing PII *(Each row refers to a grouping of databases associated with a single server)*	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Provide Names of Applicable Sites***
OITWRJSQL016: • WRJ_BIOPOINT_P16 • Censis_Beta_V2_Global • censis_graphics • Censis_HL1307 • Censis_SG1307 • NuanceMC • QCDAO	Yes	Yes	Yes	Name, SSN, DOB, Patient Demographics, Medical Record Information	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	White River Jct. VAMC
OITWRJSQL001: • AutoStoreAudit • RightFax	Yes	Yes	Yes	Name, SSN, DOB, Patient Demographics, Medical Record Information	To provide and manage benefits for the veteran	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with	White River Jct. VAMC

Components of the Area Boundary collecting/storing PII (*Each row refers to a grouping of databases associated with a single server****)***	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Provide Names of Applicable Sites***
						restricted access controls	
OITWRJSQL019: • DssDb • EMR • OAHDatabaseCore	**Yes**	**Yes**	**Yes**	Name, SSN, DOB, Patient Demographics, Medical Record Information	To provide and manage benefits for the veteran	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	White River Jct. VAMC
OITWRJAPPDSS • ICB/DocMgr/DRM/TRM	**Yes**	**Yes**	**Yes**	Name, SSN, DOB, Patient Demographics, Medical Record Information	To provide and manage benefits for the veteran	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	White River Jct. VAMC
VHAWRJWEB1 • VistA RO	**Yes**	**Yes**	**Yes**	Name, SSN, DOB, Patient Demographics, Medical Record Information	To provide and manage benefits for the veteran	Advanced Encryption Standard (AES) 256, Server is	White River Jct. VAMC

Components of the Area Boundary collecting/storing PII (*Each row refers to a grouping of databases associated with a single server****)***	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Provide Names of Applicable Sites***
						stored in a secured environment and managed with restricted access controls	