Date PIA submitted for review:

March 11, 2021

Privacy Impact Assessment for the VA Area Boundary called:

AREA PUGET SOUND INFORMATION SYSTEM

Pacific District

Facilities Supported by the Area

Facilities Supported by the Area:
1. VA Puget Sound Health Care System - Seattle Division
2. VA Puget Sound Health Care System - American Lake Division
3. VA Puget Sound Health Care System Magnolia Campus
4. VA Puget Sound Health Care System Fed Center South Campus

---

[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.

5. Edmonds CBOC
6. Mount Vernon CBOC
7. North Olympic Peninsula CBOC
8. Olympia CBOC
9. Puyallup CBOC
10. Silverdale CBOC
11. South Sound CBOC
12. VA Puget Sound Health Care System Community Housing & Outreach Center
13. VA Puget Sound Health Care System Community Resource and Referral Center (CRRC)
14. Bellingham Vet Center
15. Everett Vet Center
16. Federal Way Vet Center
17. Lacey Outstation
18. Seattle Vet Center
19. Tacoma Vet Center
20. VBA Seattle Reginal Office
21. Tahoma National Cemetery
22. Fort Worden Post Cemetery
23. Fort Lawton Post Cemetery
24. Department of Veterans Affairs Dupont Contracting
25. Program Office: Office of Inspector General (OIG)
26. Program Office: Office of General Council (OGC)

Area Boundary Contacts:

Area Privacy Officer

Name	Phone Number	Email Address	Location
Designated Area PO: James Weivoda	206-277-5156	James.weivoda@va.gov	VAMC Seattle
Jeffery Swanberg	206-277-6039	Jeffery.E.Swanberg@va.gov	VAMC Seattle
Chiquita Charles	206-277-5156	Chiquita.Charles@va.gov	VAMC Seattle
Allison Conn	206-341-8569	ALLISON.CONN@va.gov	VBA Seattle Regional Office
Cesar Romero	206-965-3469	CESAR.ROMERO1@va.gov	VBA Seattle Regional Office

Area Information System Security Officer

Name	Phone Number	Email Address	Location
Designated Area ISSO: Yosief Fesseha	206-639-3474	Yosief.Fesseha@va.gov	Puget Sound Area
Sharon Lepage-Erwin	206-764-2588	Sharon.LePageErwin@va.gov	Puget Sound Area
Gerry Ambalada	253-486-6767	Gerry.Ambalada@va.gov	Puget Sound Area
Benjamin Krueger	206-716-5728	Benjamin.Krueger@va.gov	Puget Sound Area

Area Manager

Name	Phone Number	Email Address	Location
Bruce Gibson	206-277-1127	Bruce.Gibson2@va.gov	Puget Sound Area

Abstract

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

Area Puget Sound is an Information Systems Boundary that consists of VA Puget Sound Health Care System - Seattle Division, VA Puget Sound Health Care System - American Lake Division, VA Puget Sound Health Care System Magnolia Campus, VA Puget Sound Health Care System Fed Center South Campus, Edmonds CBOC, Mount Vernon CBOC, North Olympic Peninsula CBOC, Olympia CBOC, Puyallup CBOC, Silverdale CBOC, South Sound CBOC, VA Puget Sound Health Care System Community Resource and Referral Center (CRRC), Bellingham Vet Center, Everett Vet Center, Federal Way Vet Center, Lacey Outstation, Seattle Vet Center, Tacoma Vet Center, VBA Seattle Reginal Office, Tahoma National Cemetery, Fort Worden Post Cemetery, Fort Lawton Post Cemetery and Department of Veterans Affairs Dupont Contracting. The Area Boundary environment consists of components such as workstations, laptops, portable computing devices, terminals, servers, printers, and IT enabled networked medical devices that are owned, managed, and maintained by the facilities.

The Area Boundary environment consists of components such as workstations, laptops, portable computing devices, terminals, servers, printers, and IT enabled networked medical devices that are owned, managed, and maintained by the facilities.

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 atdata centers, and connectivity to other systems. Network connectivity rules are enforced by VA approved baselines for router and switch configurations. The Area Boundary system environment also includes as applicable, subsystem storage utilities such as tape drives, optical drives, disk drives,network area storage (NAS), storage access networks (SAN), archival appliances, special purpose systems, and tier 2 storage solutions. The Area 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 Area Boundary employs amyriad of routers and switches that connect to the VA network. The system contains and transmits contact, personal health, military, and financial information on approximately (VBA 132,000 VHA 180,000) 321,000 total veterans, their dependents, volunteers, employees, and contractors.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the readerthe 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 agencymission.*
- *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 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 BenefitsManagement System, SharePoint, VistA, etc. used by the facilities to collect, use,*

disseminate, maintain, or create PII/PHIPII/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?*
  - *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy ofdata held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?*
- *What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the Cloud Service Provider or its customers (VA) be affected?*

The Area Puget Sound Information System conducts a variety of information sharing both internal and external to the Department of Veterans Affairs. Internal sharing, discussed in greater detail in Section4 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. For example, we share patient data with the VA Veterans Benefits Administration (VBA), VA Heath Eligibility Center (HEC), and Consolidated Patient Account Center (CPAC), in addition to other VA departments and programs. External sharing, which is discussed in greater detail in Section 5 of this PIA, is done for several reasons with the Social Security Administration, state health and veteran agencies, and other agenciesand organizations. The following VA System of Record Notices (SORNs) apply to the Area Puget Sound Information System:

The legal authorities include Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Privacy Act of 1974. Also 38 U.S. Code Chapter 77 and Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b).

In order to help fulfill the responsibilities of the VBA, the Puget Sound Regional Office uses the Area Puget Sound Information System to assist in serving 1,000,000 to 9,999,999 veterans and their dependents. The Area Puget Sound Information System consists of file servers, routers, printers, and networked PCs which allow for the processing and storage of data necessary for carrying out VBA functions. The Area Puget Sound Information System does not directly host or maintain any major VA systems or applications. Any data stored on the system is the result of employees directly storing or maintaining data, such asExcel Spreadsheets or Word Documents, on the network. Although the majority of veteran data is stored in a central database not located at this facility, during the processing of benefits, it is often necessary for employees to store files containing personal information on the network. This is donefor a variety of reasons to include but not limited to temporary storage while working a case, for reference purposes, or to assist in case management. Any potential records created, maintained, orstored on the Area Puget Sound Information System are governed by Veterans Affairs System of Record Notice (VA SORN) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28 (July

19, 2012). The Area Puget Sound Information System connects directly to the VA Enterprise wide-area network, maintained by the VA Network Security Operations Center (NSOC). This allows select users at the Veterans Affairs Medical Centers (VAMCs) limited access to a web based Hospital Inquiry database known as Web-HINQ, and Veterans Information Solution (VIS), which are used to verify Veteran eligibility for benefits, and Veterans Benefits Management System (VBMS), which is used to processVeteran disability claims. Users with the Washington Department of Veterans Services and the Disabled American Veterans are provided read only access to Control of Veteran Records (COVERS), Share, a Microsoft Windows®-based application which is utilized by the Regional Offices (RO) to access the Beneficiary Inquiry Records Locator System (BIRLS), Compensation and Pension (C&P) MasterRecords, Pending Issue File (PIF), Payment History File (PHF), Corporate database, Social Security Administration, and COVERS records. SHARE T-11 provides a single computing system with data sources located on different databases in multiple locations. Veterans Appeals Control and Locator System (VACOLS), Virtual VA, VBMS and Modern Award Processing (MAP-D), an application to help perform proper claims development. However, no major applications are supported by this system. All of the major applications are supported and located at various sites throughout the UnitedStates, and the local Area Puget Sound Information System only accesses the applications through the network. The Area Puget Sound Information System simply hosts the client portion of each client-servermajor application.

The Veteran claims information is either entered manually from paper submitted forms or transferred electronically frominformation entered through the web based eBenefits portal. Thesystem is not a regional system.

The completion of this PIA will not result in any business or technology changes for the area.

The applicable SORs for Area Puget Sound Information System include:

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	Applicable SORs
VHA	- Non-VA Fee Basis Records-VA, SOR 23VA10NB3 - Non-VA Fee Basis Records-VA, SOR 23VA16 - Patient Medical Records-VA, SOR 24VA10P2 - Veteran, Patient, Employee, and Volunteer Research and DevelopmentProject Records- VA, SOR 34VA12 - Community Placement Program-VA, SOR 65VA122 - Health Care Provider Credentialing and Privileging Records-VA¸SOR77VA10Q - Health Care Provider Credentialing and Privileging Records-VA¸SOR77VA10A4 - Health Care Provider Credentialing and Privileging Records-VA¸SOR77VA111 - Veterans Health Information Systems and Technology Architecture

Site Type: VBA/VHA/NCA or Program Office	Applicable SORs
	(VistA) Records-VA, SOR 79VA10P2 • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA19 • Enrollment and Eligibility Records-VA SORN 147VA16 • Healthcare Eligibility Records – VA SORN 89VA19 • Income Verification Records-VA, SOR 89VA10NB • Automated Safety Incident Surveillance and Tracking System-VA, SOR99VA13 • The Revenue Program Billings and Collection Records-VA, SOR 114VA16 • National Patient Databases-VA, SOR 121VA19 • VHA Corporate Data Warehouse- VA 172VA10P2 • Freedom of Information Act (FOIA) Records-VA SORN 119VA005R1B/C • Patient Advocate Tracking System (PATS)-VA SORN 100VA10N10 • Voluntary Service Records-VA SORN 57VA135
VBA	• Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28 • Veterans and Beneficiaries Identification Records Location Subsystem-VA SORN 38VA23 • Veterans and Beneficiaries Identification Records Location Subsystem-VA SORN 38VA21 • Veterans Assistance Discharge System-VA SORN 45VA21 • Principles of Excellence Centralized Complaint System – VA SORN 170VA22 • Beneficiary Fiduciary Field System (BFFS)-VA SORN 37VA27
NCA	• Veterans (Deceased) Headstone or Marker Records-VA SORN 48VA40B • Veterans and Dependents National Cemetery Gravesite Reservation Records -VA SOR 41VA41 • VA National Cemetery Pre-Need Eligibility Determination Records -VA SOR 175VA41A
Vet Centers	• Patient Medical Records-VA, SOR 24VA10P2

Site Type: VBA/VHA/NCA or Program Office	Applicable SORs
Program Office Office of Inspector General (OIG)	• Criminal Investigations-VA SORN 11VA51 • The Office of Inspector General Management Information System (MIS)-VA SORN 71VA53
Program Office Office of General Council (OGC)	• The Office of Inspector General Management Information System (MIS)-VA SORN 140VA02REG • General Counsel Legal Automation Workload System (GCLAWS)-VA SORN 144VA026 • Litigation Files-VA SORN 16VA026

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:

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

Other personal information accessible through the Area Puget Sound Information System may include:

Next of Kin Guardian Information, ePHI, Employment information, Veteran dependent information Disclosure requestor information, Death certificate information, Tumor PII/PHI Statistics, Criminal background information, Education information, Gender, bank account information, gross income and net worth Information, Military History/Service Connection Service-connected disabilities, (e.g., name, service number, date of birth, rank, sex, total amount of active service, branch of service, character of service, pay grade, assigned separation reason, service period, whether veteran was discharged with a disability, reenlisted, received a Purple Heart or other military decoration); payment information (e.g., Veteran payee name, address, dollar amount of readjustment service pay, amount of disability or pension payments, number of non-pay days, any amount of indebtedness (accounts receivable) arising from title 38 U.S.C. benefits and which are owed to the VA); medical information (e.g., medical and dental treatment in the Armed Forces including type of service-connected disability, medical facilities, or medical or dental treatment by VA health care personnel or received from private hospitals and health care personnel relating to a claim for VA disability benefits or medical or dental treatment); personal information(e.g., marital status, name and address of dependents, occupation, amount of education of a Veteran or a dependent, dependent's relationship to veteran); education benefit information (e.g., information arising from utilization of training benefits such as a veteran trainee's induction, reentrance or dismissal from a program or progress and attendance in an education or training program); applications for compensation, pension, education and vocational rehabilitation benefits and training which may contain identifying information, military service and active duty separation information, payment information, medical and dental information, personal and education benefit information relating to a veteran or beneficiary's incarceration in a penal institution (e.g.), name of incarcerated Veteran or beneficiary, claims folder number, name and address of penal institution, date of commitment, type of offense, scheduled release date, Veteran date of birth, beneficiary relationship to

Veteran and whether Veteran or beneficiary is in a work release or half-way house program, on parole or has been released from incarceration), etc.

PII Mapping of Components

Area Puget Sound Information System consists of 41 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 Area Puget Sound Information System and the reasons for the collection of the PII are in the **Mapping of Components Table in <u>Appendix B</u> 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 that resides within the facilities in the Area Boundary is collected, maintained, and/or disseminated 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.

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

The information that resides on the Information System is collected or maintained and/or disseminated by the Puget Sound VA Medical Center and/or Puget Sound Regional Office, comes from a variety of sources to include from veteran or patients, from programs and resources to include VA Health Eligibility Center (HEC), Department of Defense (DoD), VA Network Authorization Office (NAO), non-VA Care payments, and non-VA medical providers. 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.

The Puget Sound Regional Office employs the following information sources:

- Loan Guarantee Home, Condominium and Manufactured Home Loan Applicant Records
- Specially Adapted Housing Applicant Records, and Vendee Loan Applicant Records
- 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. 53VA00 Veterans Mortgage Life Insurance
- VA, Veterans and Beneficiaries Identification and Records Location (BIRLS)
- Compensation, Pension, Education, and Rehabilitation (covers BDN and Corporate databases)

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 controlnumber and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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), orinterviews 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 medicalrecord 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 viathe Department of Treasury. The VBA toll free number for veterans is 1-800-827-1000. Clientsare 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.
NCA	Information may be collected directly from family of the deceased

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](#).

Information from outside resources comes to the Area Puget Sound Information System using several methods such as Fax, physical mail, email, secure web portal, VPN connection, Citrix Access Gateway, secure file transfer, and courier. Chief among these sources, are the DoD, SSA, and IRS. The DoD provides military records, including medical records compiled when the patient was a member of the US Military. Income information is verified using information from the Social Security Administration (SSA) and the Internal Revenue Service (IRS).

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 sh ould 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.

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.

Site Type: VBA/VHA/NCA or Program Office	Purpose of Information Collection
	Information is collected to provide all entitled benefits in the most complete and effective manner.
NCA	• To determine eligibility for burial benefits Crave Location

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

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 thisprocess 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 that is collected and used directly from enterprise systems have additional details regarding checksforaccuracy in their own enterprise level PIAs.

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 accuratebecause it is provided directly by the individual. Additionally, information entered an individual's medical record by a doctor or other medical staff is also assumed to be accurate and is not verified.

Information is checked through the VBA to verify eligibility for VA benefits. Information about military servicehistory is verified against official DoD military records and income information is verified using information from the Social Security Administration (SSA) and the Internal Revenue Service (IRS).

Employee, contractor, student and volunteer information is obtained by automated tools as well as obtaineddirectly by the individuals. The Federal Bureau of Investigation and Office of Personnel Management are contacted to obtain background reviews. Provider credentialing information is obtained from a variety of education resources.

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 Federallaws, regulations, statutes, and Executive Orders.

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

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104 -191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code); 45 Code of Federal Regulations (C.F.R). parts 160 and 164(HIPAA Privacy and Security Rules). Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111 -5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.

Legal Authority Table

Site Type: VBA/VHA/NCA or Program Office	Legal Authority
VHA	• 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) • 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. • Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code); 45 Code of Federal Regulations (C.F.R). parts 160 and 164 (HIPAA Privacy and Security Rules). • Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb.17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.
VBA	• Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), Generally, the authority to operate the Veterans Benefit Administration come from 38 U.S. Code Chapter 77. • Specific authority to operate the Area Puget Sound Information System is Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55. This information is reflected in the VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28 (July 19, 2012).
NCA	• *38 U.S.C. § 2411, 38 U.S.C. § 2402*

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.

Follow the format below when entering your risk assessment:

Privacy Risk:
VA Area Puget Sound Information System collects Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

Mitigation:
The Area Puget Sound Information System employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control, awareness and training, audit and accountability, certification, accreditation, and security assessments; configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and system and information integrity. The area employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

All employees with access to Veteran's health information are required to complete the Privacy and HIPAA Focused training as well as the VA Privacy and Information Security Awareness & Rules of Behavior training annually. The VA enforces two-factor authentication by enforcing smartcard logon requirements. PIV cards are issued to employees, contractors, and partners in accordance with HSPD-12. The Personal Identity Verification (PIV) Program is an effort directed and managed by the Homeland Security Presidential Directive 12 (HSPD- 12) Program Management Office (PMO). IT Operations and Services (ITOPS) Solution Delivery (SD) is responsible for the technical operations support of the PIV Card Management System. Information is not shared with other agencies without a Memorandum of Understanding (MOU) or other legal authority.

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.

- **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 contactperson.
- **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 Policeinvestigations.
- **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. HighSchool 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 assistingin 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 lawenforcement 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 whatwill 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 Area Puget Sound Information System uses statistics and analysis to create general reports

that provide theVA a better understanding of *patient care, benefits, Veteran 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.

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, feeservices, etc.
- Daily bed management activity
- Coding averages for outpatient/inpatient encounters
- Satisfaction of Healthcare Experience of Patients (SHEP) data as it pertains to customer satisfactionregarding 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 onpaper 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 forassuring safeguards for the PII/PHI?

Describe any types of controls that may be in place to ensure that information is handled in accordance with theuses 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 ifan 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 theproject?

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

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

administrative rounds during which personal examine all areas within the facility to ensure information is being appropriately used and controlled.

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 Area Puget Sound Information System Boundary itself, does retain information.

- 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

The Veteran records are transferred to 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.

Some claims folders are electronically imaged; in which case, the electronic folder is maintained in the same manner as the claims folder.

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 maximum entitlement or upon the exceeding of a Veteran 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 or burning.

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.
Yes

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 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

Site Type: VBA/VHA/NCA or Program Office	Length of Retention
	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.

The Area Puget Sound Information System retains patient health record in accordance to applicable record control guidelines: Department of Veterans Affairs, Veteran Health Administration Record Control Schedule (RCS) 10-1.

These documents specify how long records will be retained by the VA, if/when they will be transferred to anational 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 Veterans' Health Administration, please review RCS-10and RCS-005-1.

Below are some key record retention schedules for your information:

Medical Records Folder File or CHR (Consolidated Health Record): These records contain all professionaland administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a Federal records storage facility. Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs RecordControl Schedule (RCS)-10, Part Three, Chapter Six- Healthcare Records, Item 6000.1a. and 6000.1d.(January 2016)).

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 afterseparation from Federal service. (Department of Veterans Affairs Record Control Schedule (RCS)-10, Part Two, Chapter Three- Civilian Personnel, Item No. 3000.1 (January 2016)).

Financial Records: Different forms of financial records are retained 1-7 years based on specific retentionschedules. Please refer to VA Record Control Schedule (RCS)-10, Part Two, Chapter Four- Finance Management (http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf) for specific guidelines.

Office if Information & Technology (OI&T) Records: These records are created, maintained and disposed ofin accordance with Department of Veterans Affairs, Office of Information & Technology RCS 005-1 (August 3, 2009). Please refer to VA Records Control Schedule (RCS)-05 (http://www.oprm.va.gov/docs/RCS005-1-OIT- 8-21-09.pdf) forspecific guidelines.

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.

Retention Schedule Table

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

The Area Puget Sound Information System uses 2 NARA approved retention schedules: Department of Veterans Affairs, Veterans Health Administration Records Control Schedule 10-1 (November 2017) https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

Department of Veterans Affairs, Office of Information & Technology Record Control Schedule 005-1 (Aug 3, 2009). https://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf

Records Control Schedule VB-1 Part 1, Section, XIII, Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc

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 Area Puget Sound Information System is destroyed by the disposition guidance of RCS 10-1, and VA Directive 6500. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014)

Additionally, the *Area Puget Sound Information System* 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. *OIT/OIS SOP MP-6 Electronic Media Sanitization V4.0 is also used as guidance.*

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 Veterans' Affairs Directive 6500 VA Cybersecurity**

Program (January 23, 2019). When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Directive 6500. Digital media is shredded or sent out for destruction per VA Directive 6500.

Paper records are shredded on-site by a shredding company, and a certificate of destruction is sent to the facility. 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

Controls for protecting PII used for testing, training and research for IT system development and deployment are often security controls if the PII is electronic. When paper PII, reasonable safeguards for protecting the PII are to be employed. For training purposes, test patients are used and not actual active Veteran PII or PHI is used. If paper documents are required for training purposes, information is redacted out by the facility Privacy Officer.

The Puget Sound Regional Office does not conduct research or testing activities. Locally developed presentations for training purposes, that may become publicly available, do not contain PII per VA Directive 6511, and are reviewed by the Puget Sound Regional Office Privacy Officer. Training is also conducted locally for Veterans Service Center (VSC) employees with oversight from VBA's Compensation Service Training. Types of data used by VBA include limited data sets, with mock information (no live claims data) or de-identified information, with all PII removed. This training utilizes approved and controlled access to the Veterans Benefits Management System (VBMS) in "Demonstration Mode", which contains dummy information and is not connected to live claims information. Additionally, live claims information is not presented in recorded environments; PII is not exposed to non-VA personnel. All training access is documented using controlled access with a unique student number and pseudo-claim numbers assigned.

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 retainedonly 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 longerrelevant 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 maintained by Area Puget Sound Information System could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greaterrisk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation: To mitigate the risk posed by information retention, Area Puget Sound Information System adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. The Area Puget Sound Information System ensures that all personnel involved with the collection, use and retention of dataare trained in the correct process for collecting, using and retaining this data. A Records Management Officer (RMO), Privacy Officer (PO) and an Information System Security Officer (ISSO) are assigned to the area to ensure their respective programs are understood and followed by all to protect sensitive information form the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls thatoverlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning the proper handlingof information.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.NOTE: Question 6 on Privacy Threshold Analysis should be used to answer this question.

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?

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization orIT 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 citationto 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, orby some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

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

Data Shared internally by facilities within the Area including VA Enterprise Systems Organizations

List the Program Office or IT Area Boundary information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary	Describe the method of transmittal	Provide nameof Applicable Area Sites)
VA National Cemetery Administration (NCA)	Death/BurialBenefit	Death certificates, veteran eligibility.	Electronically, verbal or written. Information may be transmitted upon request in an electronic (encrypted email/mailing of encrypted CD's), written (facsimile or FEDEX/USPS/UPS) or verbal format based on the individual request.	Area Puget Sound
VA Network Authorization Office	Health Care	Demographics, diagnoses, medical history, service connection, provider orders, VHA recommendation/approval for non-VA care.	Fee Basis Claim System (FBCS) authorization software program.	Area Puget Sound
Veterans Benefits Administration	Determine Veteran eligibility and Benefits	Personally, Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	Compensation and Pension Record Interchange (CAPRI) electronic software package. Information may be transmitted electronically. AAC employees	Area Puget Sound

List the Program Office or IT Area Boundary information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary	Describe the method of transmittal	Provide nameof Applicable Area Sites)
			may have access to log into CPRS or VistA	
Veterans Health Administration	Health/medical payment authorization	System Log files, sample clinical data that may contain Protected Health Information (PHI) appropriate to the agreements	Electronically pulled from VistA thru Computerized Patient Record System (CPRS)	Area Puget Sound
Data Services	Data Services	Personally, Identifiable Information (PII), Protected Health Information (PHI), Individually Identifiable Information (III), System Log files, sample clinical data that may contain Protected Health Information (PHI)	SOAP over HTTPS using SSL encryption and Certificate exchange	VAMC Puget Sound
Austin Automation Center (AAC)	Data Services	Name, Date of Birth, Sex, SSN, demographics and health information	Information may be transmitted electronically. AAC employees can log into CPRS or VistA	Area Puget Sound
Department of Veterans Affairs General Counsel	Legal	VHA may provide all information, including individually-identifiable information and 38 U.S.C. 7332 information for any official purpose authorized by law. Pertinent Personally Identifiable Information (PII)	Information may be transmitted electronically thru encrypted emails, mail of encrypted CDs, secure facsimile, via secure web portal or hard copies via routine mail, written or verbal format based on the individual request.	Area Puget Sound

List the Program Office or IT Area Boundary information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary	Describe the method of transmittal	Provide nameof Applicable Area Sites)
		such as Name, SSN, DOB, financial information; Protected Health Information (PHI), and Individually Identifiable Information (III) appropriate to the request		
VA Research	Research	Pertinent PII, PHI, and III appropriate to the request (each research project have an IRB data plan	Information may be transmitted electronically SFTP thru encrypted emails, mail of encrypted CDs, secure facsimile, via secure web portal or hard copies via routine mail, written or verbal format based on the individual request. copies via routine mail, written or verbal format based on the individual request.	VAMC Puget Sound
VA Tumor Register	Tracking & Trending of Disease Progression	Name, demographics, Protected Health Information (PHI), Veteran eligibility	Hard copy sent through the mail	VAMC Puget Sound
VA HIV Register	Tracking & Trending of Disease Progression	Name, Date of Birth, Sex, SSN, demographics and health information	Information may be transmitted electronically. AAC employees can log into CPRS or VistA	VAMC Puget Sound
VA Network Authorization office - NON-VA Care Payments	Health/medical payment authorization	Death certificates, veteran eligibility	Hard copy sent through the mail	VAMC Puget Sound

List the Program Office or IT Area Boundary information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary	Describe the method of transmittal	Provide nameof Applicable Area Sites)
Consolidated Patient Account Center	Health/medical payment authorization	Diagnosis, service connection, dates of service, health insurance information, demographics	Electronically pulled from VistA thru CPRS	VAMC Puget Sound
VA Health Eligibility Center	Determine Veteran eligibility	Service dates, SSN, demographics, service connection	Scanned documents uploaded into shared programs	Area Puget Sound
MyHealthe Vet	Health Care	Personally, Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	Electronically pulled from VistA	VAMC Puget Sound
Occupational Health Employee Record System (OHRES)	Health Care fitness for duty	Personally, Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	Employee Health staff access to VISTA and CPRS.	VAMC Puget Sound

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 internal sharing of data is necessary individuals to receive benefits at the Area Puget Sound Health System. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintendedparties or recipients.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employeesecurity and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within thefacilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VApersons or processes acting on behalf of VA persons is to be requested or granted.

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: This question is #7 in the Privacy Threshold Analysis.

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.

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures inplace to secure data	List name of Applicable Area Sites
Axiom Coding	Diagnosis, service connection, dates of service, health insurance information, demographics. Medical care cost recovery/payment	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III). Appropriate to the agreement on the (ISA/MOU/BAA)	National ISA/MOU Title 38, United StatesCode, Section 5701	Site to Site	VAMC Puget Sound
Washington State Health and Human Services	Relating to abuse, neglect or exploitation of vulnerable adults.	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI),and Individually Identifiable Information (III) appropriate to the agreement.	VA SORN 24VA10A7 Standing Leter	Fax	VAMC Puget Sound
Veterans Command Transcription Service	Transcription services connection, dates of service, health notes	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually	National ISA/MOU Title 38, United StatesCode, Section 5701	Site to Site	VAMC Puget Sound

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data	List name of Applicable Area Sites
		Identifiable Information (III). Appropriate to the agreement on the (ISA/MOU/BAA)			
Federal Bureau of Investigations (FBI)	Crimes, fugitive felon program.	Name, Date of Birth, Sex, SSN, Demographics, Pertinent PII.	VA SORN02VA135 VA SORN 79VA19	Electronic via FBI website	Area Puget Sound
GE Med-IT, General Electric	Biomedical data	Pertinent Personally Identifiable Information (PII),Protected Health Information (PHI),and Individually Identifiable Information (III). Appropriate to theagreement on the (ISA/MOU/BAA)	National ISA/MOU	Site to Site	VAMC Puget Sound
Office of Personnel Management (OPM)	Assistance in employment and personal identity – conducting computer	Pertinent Personally Identifiable Information (PII), Protected Health Info(PHI), and	National ISA/MOU SORN 58VA21/22/28 (July 19, 2012)	Site to Site	Area Puget Sound

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data	List name of Applicable Area Sites
	matching program	Individually Identifiable Info. Per agreement.			
Abbott Laboratories	Facilitate healthcare services for Veterans	System Log files, sample clinical data that may contain Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	National ISA/MOU	Site to Site	VAMC Puget Sound
AGFA	Employee Representation	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III), Appropriate to the agreement on the (ISA/MOU/BA	VA SORN 24VA10A7 VA Contract	Site to Site	VAMC Puget Sound

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures inplace to secure data	List name of Applicable Area Sites
		A			
ALERE	Facilitate healthcare servicesfor Veterans	System Log files, sample clinical data that may contain Pertinent Personally Identifiable Information (PII),Protected Health Information (PHI),and Individually Identifiable Information (III).	National ISA/MOU	Site to Site	VAMC Puget Sound
Carefusion	Diagnosis, service connection, dates of service, health insurance information, demographics.	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III). Appropriate to the agreement on the (ISA/MOU/BAA)	National ISA/MOU Title 38, United StatesCode, Section 5701	Site to Site	VAMC Puget Sound
OLYMPUS	Facilitate healthcare	System Performance	National ISA/MOU	Site to Site	VAMC Puget Sound

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures inplace to secure data	List name of Applicable Area Sites
	servicesfor Veterans	Parameters / System Monitoring information, which may include but are not limited to disk usage, reconstruction speed, image quality parameters, Helium levels, temperature, humidity.			
Omnicell	Facilitate healthcare servicesfor Veterans	Pertinent Personally Identifiable Information (PII),Protected Health Information (PHI),and Individually Identifiable Information (III). Appropriate to theagreement on the (ISA/MOU/BAA)	National ISA/MOU	Site to Site	VAMC Puget Sound
Quest Diagnostic National	Facilitate healthcare servicesfor Veterans	System Log files, sample clinical data that may contain	National ISA/MOU	Site to Site	VAMC Puget Sound

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures inplace to secure data	List name of Applicable Area Sites
		Pertinent Personally Identifiable Information (PII),Protected Health Information (PHI),and Individually Identifiable Information (III).			
EPIC	Medical Record interface	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III), Appropriate to the agreement on the (ISA/MOU/BAA	National ISA/MOU	Site to Site	VAMC Puget Sound
Phillips	Facilitate healthcare servicesfor Veterans	System Performance Parameters / System Monitoring information, which may include but are	National ISA/MOU	Site to Site	VAMC Puget Sound

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures inplace to secure data	List name of Applicable Area Sites
		not limited to disk usage, reconstruction speed, image quality parameters, Helium levels, temperature, humidity.			
Roche	Facilitate healthcare services for Veterans	Personally Identifiable Information (PII),Protected Health Information (PHI),and Individually Identifiable Information (III).	National ISA/MOU	Site to Site	VAMC Puget Sound
ScriptPro	Facilitate healthcare servicesfor Veterans	Prescription data that may include PII/PHI, Non-identifiable Information, Limited Data Set, De-identified Information, Patient Identifiers and Unique Identifier from the Script-Pro SP Central system	National ISA/MOU	Site to Site	VAMC Puget Sound

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data	List name of Applicable Area Sites
Siemens	Facilitate healthcare services for Veterans	Software updates and patches to Operating system, applications and antivirus update of definition files.	National ISA/MOU	Site to Site	VAMC Puget Sound
Swisslog	Facilitate healthcare services for Veterans	Pertinent Personally Identifiable Information (PII),Protected Health Information (PHI),and Individually Identifiable Information (III). Appropriate to the agreement on the (ISA/MOU/BAA)	National ISA/MOU	Site to Site	VAMC Puget Sound
Topcon	Facilitate healthcare services for Veterans	Pertinent Personally Identifiable Information (PII),Protected Health Information (PHI),and Individually Identifiable Information (III).	National ISA/MOU	Site to Site	VAMC Puget Sound

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data	List name of Applicable Area Sites
		Appropriate to the agreement on the (ISA/MOU/BAA)			
Vecna	Facilitate healthcare services for Veterans	System Log files, sample clinical data that may contain Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	National ISA/MOU	Site to Site	VAMC Puget Sound
National Crime Information Center	Reportable crimes/information on National Crimes committed.	Pertinent Personally Identifiable (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) appropriate to the agreement.	National ISA/MOU	ILETS Terminal- Washington Law Enforcement Terminal/Site to Site.	VAMC Puget Sound
Social Security	Benefits and entitlement	Name: Social Security Number:	Information Exchange	Electronic transmission	Area Puget Sound

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data	List name of Applicable Area Sites
Administration/Disability	verification/ Payment/disability benefits	Date of Birth: Mailing Address: Zip Code: Phone Numbers: Email Address: Emergency Contact Information: Financial Account Information: Health Insurance Beneficiary Numbers Current Medications: Previous Medical Records	Agreement #384 Between the Department of Veterans Affairs, Veterans Benefits Administration and the Social Security Administration Title 38, United States Code, Section 5701; SORN 79VA19	via web-based applications not hosted on Area Puget Sound Information System.	
Internal Revenue Service	Income and Debt Verification	Name: Social Security Number: Date of Birth: Mailing Address: Zip Code: Phone Numbers: Email Address: Emergency Contact Information: Financial Account Information:	SORN 58VA21/22/28 (July 19, 2012)	Electronic transmission methods through VA network connected computers	Area Puget Sound

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data	List name of Applicable Area Sites
Social Security Administration / Disability	Benefits and entitlement verification/ Payment/disability benefits	Name: Social Security Number: Date of Birth: Mailing Address: Zip Code: Phone Numbers: Email Address: Emergency Contact Information: Financial Account Information: Health Insurance Beneficiary Numbers Current Medications: Previous Medical Records	Information Exchange Agreement #384 Between the Department of Veterans Affairs, Veterans Benefits Administration and the Social Security Administration Title 38, United States Code, Section 5701; SORN 79VA19	Electronic transmission via web-based applications not hosted on Area Puget Sound Information System.	Area Puget Sound
Department of Labor	Conduct a computer matching program	Pertinent Personally Identifiable (PII), disability and award type	SORN 58VA21/22/28 (July 19, 2012)	Electronic transmission methods through VA network connected computers	Area Puget Sound

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data	List name of Applicable Area Sites
Department of Treasury	Conduct a computer matching Program	Pertinent Personally Identifiable (PII), disability and awardtype	SORN 58VA21/22/28 (July 19,2012)	Electronic transmission methods through VA network connected computers	Area Puget Sound
Federal Bureau of Prisons	Conduct a computer matching program	Pertinent Personally Identifiable (PII), disability and awards type	SORN 58VA21/22/28 (July 19, 2012)	Electronic transmission methods through VA network connected computers	Area Puget Sound
Department of Health and Human Services	Conduct a computer matching program	Pertinent Personally Identifiable (PII), disability and awardtype	SORN 58VA21/22/28 (July 19, 2012)	Electronic Transmission methods through VA network connected computers	VAMC Puget Sound
Defense Manpower Data Center	Conduct a computer matching program	Pertinent Personally Identifiable (PII), disability and awardtype	SORN 58VA21/22/28 (July 19, 2012)	Electronic transmission methods through VA network connected computers	Area Puget Sound
Federal Parent Locator System, Department of Treasury	Conduct a computer matching program	Pertinent Personally Identifiable (PII), disability and awardtype	SORN 58VA21/22/28 (July 19, 2012)	Electronic transmission methods through VA network connected computers	VARO Puget Sound

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data	List name of Applicable Area Sites
General Accounting Office	Conduct a computer matching program	Pertinent Personally Identifiable (PII), disability and award type	SORN 58VA21/22/28 (July 19, 2012)	Electronic transmission methods through VA network connected computers	Area Puget Sound
Veterans Mortgage Life Insurance	Conduct a computer matching program	Pertinent Personally Identifiable (PII), disability and award type	SORN 58VA21/22/28 (July 19, 2012)	Electronic transmission methods through VA network connected computers	VARO Puget Sound
Office of Inspector General	Conduct a computer matching program	Pertinent Personally Identifiable (PII), disability and award type	SORN 58VA21/22/28 (July 19, 2012)	Electronic transmission methods through VA network connected computers	Area Puget Sound
Bureau of Census	Conduct a computer matching program	Pertinent Personally Identifiable (PII), disability and award type	SORN 58VA21/22/28 (July 19, 2012)	Electronic transmission methods through VA network connected	Area Puget Sound
Bureau of Census	Conduct a computer matching program	Pertinent Personally Identifiable (PII), disability and award type	SORN 58VA21/22/28 (July 19, 2012)	Electronic transmission methods through VA network connected	Area Puget Sound
Department of Housing and Urban Development	Conduct a computer matching program	Pertinent Personally Identifiable	SORN 58VA21/22/28 (July 19, 2012)	Electronic Transmission methods through VA	Area Puget Sound

List External Program Office or IT Area Boundary information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary	List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary	List the legal authority, binding agreement, SORN routineuse, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data	List name of Applicable Area Sites
		(PII), disability and award type		network connected computers	
IDVS/DAV, Veterans Service Organizations; Accredited Claims Representatives; Private Attorneys	Assist Veterans with filing benefit claims.	Read only access to Covers, Share, VACOLS, Virtual VA, VBMS and MAP-D	SORN 58VA21/22/28 (July 19, 2012)	Electronic transmission methods through Citrix Access Gateway (CAG)	VARO Puget Sound
Seattle Institute for Biomedical and Clinical Research	Research Administration	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), Individually Identifiable Information (III), System Log files, sample clinical data that may contain PHI appropriate to the agreements (MOU ISA and BAA)	VA SORN 24VA10A7	Electronic transmission methods through VA network-connected computers	VAMC Puget Sound

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

The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-

60. As partof the categorization any PII is identified.

The VA has policies which direct and guide the activities and processes performed by the VA. The policies areperiodically 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, ortransmitted between IT centers.

Internal protection is managed by access controls such as user authentication (user IDs, passwords and PersonalIdentification 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 ofthe original collection.

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

Follow the format below:

Privacy Risk: The sharing of data is necessary for individuals to receive benefits at the Area Puget Sound InformationSystem. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: Safeguards implemented to ensure data is not shared inappropriately with organizations are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need to know purposes, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption and access authorization are all measures that are utilized within the administrations. Standing letters for information exchange, Business Associate Agreements (BAA) and memorandums ofunderstanding between agencies and VA are monitored closely by the Privacy Officer (PO), ISSO to ensure protection of information.

All personnel accessing Veteran's information must first have a successfully adjudicated background screeningor Special Agreement Check (SAC). This background check is conducted by the Office of Personnel Management A background investigation is required commensurate with the individual's duties.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, theright 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 ofthe notice in <u>Appendix A</u>. (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 FederalRegister, 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 andPrivacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

The Area Puget Sound Information System provides notice of information collection in several additional ways. The initial method of notification is in person during individual interviews or in writing via the Privacy Act statement on forms and applications completed by the individual. Additionally, the Department of Veterans Affairs also provides notice by publishing the following <u>VA System of Record Notices</u> (VA SORN) in the Federal Register and online.

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	Applicable SORs
VHA	• Non-VA Fee Basis Records-VA, SOR 23VA10NB3 • Patient Medical Records-VA, SOR 24VA10P21 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA12 • Community Placement Program-VA, SOR 65VA122 • Health Care Provider Credentialing and Privileging Records-VA¸SOR 77VA10E2E • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10P2 • Income Verification Records-VA, SOR 89VA10NB

Site Type: VBA/VHA/NCA or Program Office	Applicable SORs
	• Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA131 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10D • National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147-VA10NF1 VHA Corporate Data Warehouse- VA 172VA10P2
VBA	• Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28
NCA	• Veterans and Dependents National Cemetery Gravesite Reservation Records -VA SOR 41VA41 • Veterans and Dependents National Cemetery Interment Records-VA SOR 42VA41 • VA National Cemetery Pre-Need Eligibility Determination Records - VA SOR 175VA41A

This Privacy Impact Assessment (PIA) also serves as notice of the Area Puget Sound Information 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 VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans.

The following Written notice is on all VA forms: PRIVACY ACT INFORMATION: No allowance of compensation or pension may be granted unless this form is completed fully as required by law (38 U.S.C.5101). The responses you submit are considered confidential (38 U.S.C. 5701). VA may disclose the information that you provide, including Social Security numbers, outside VA if the disclosure is authorized under the Privacy Act, including the routine uses identified in the VA system of records, 58VA21/22 Compensation, Pension, Education, and Rehabilitation Records - VA. The requested information is considered relevant and necessary to determine maximum benefits under the law. Information submitted is subject to verification through computer matching.

Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.

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 Area Puget Sound Information System only requests information necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them.

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with Area Puget Sound Information System.

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

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. • Individuals have the right to consent to particular uses of information. • Individuals are directed to use the 10- 5345 Release of Information form describing what information is to be sent out and to whom it is being sent to.
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.

Site Type: VBA/VHA/NCA or Program Office	Information Consent Rights

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that veterans and other members of the public will not know that the Area Puget Sound Information System exists or that it collects, maintains, and/or disseminates PII, PHI or PII/PHI about them.

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for health care. s. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SOR) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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 andregulations 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.

An individual wanting notification or access, including contesting the record, should mail or deliver a request to theoffice identified in the SOR. If an individual does not know the "office concerned," the request may be addressed tothe PO of any VA field station VHA facility where the person is receiving care or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420. The receiving office must promptly forward the mail request received to the office of jurisdiction clearly identifying it as "Privacy Act Request" and notify the requester of the referral.

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.

Additionally, veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the my Healt*he*Vet program, VA's online personal health record. More information about myHealt*he*Vet is available at https://www.myhealth.va.gov/index.html.

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 maybe 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 beaddressed. If the correction procedures are the same as those given in question 7.1, state as much.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regardingaccess and correction procedures can be found in the notices listed in **Appendix A**.

The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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

How are individuals made aware of the procedures for correcting his or her information? This

may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist tocorrect information, if an individual is not made fully aware of the existence of those procedures, then the benefits ofthe procedures are significantly weakened.

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

Veterans are informed of the amendment process by many resources to include the VHA Notice of PrivacyPractice (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 carefacility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appealrights. In response, youmay 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 healthinformation

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

Additional notice is provided through the SORS listed in 6.1 of this PIA and through the area Release ofInformation 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.
<u>Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.</u>

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 aproject does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose ofthe 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 projectmaintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice asto 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 informationabout him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:
Privacy Risk: There is a risk that members of the public will not know the relevant procedures for gainingaccess to, correcting, or contesting theirinformation.

Mitigation: Area Puget Sound Information System mitigates the risk of incorrect information in an individual's records by authenticating information when possible using the resources discussed in question 1.5. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.

As discussed in question 7.3, the NOPP, which every enrolled Veteran receives every three years or when thereis a major change. The NOPPdiscusses the process for requesting an amendment to one's records.

The Area Puget Sound Information System Release of Information (ROI) office is available to assist Veterans withobtaining access to their health records and other records containing personal information. The Veterans' Health Administration (VHA) established MyHealthEVet program to provide Veterans remoteaccess to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Informationestablishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the Area Boundary, and are theydocumented?

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 Area Puget Sound Information System by gainful employment in the VA or upon being awarded a contract that requires access to the Area systems. Upon employment, the Office of Information & Technology (OI&T) creates computer and network access accounts as determined by employment positions assigned. Users are not assigned to software packages or network connections that are not part of their assigned duties or within their assigned work area. VA Area Puget Sound Information System requires access to the GSS be requested using the local access request system. VA staff must request access for anyone requiring new or modified access to the GSS. Staff are not allowed to request additional or new access for themselves.

Access is requested utilizing Electronic Permission Access Area Boundary (ePAS). Users submit access requests based on need to know and job duties. Supervisor, ISSO and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, 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 the facilities are protected from outside access by the Federal Protective Service or other security personnel. Access to computer rooms at VA Area Puget Sound Information System is generally limited by appropriate locking devices and restricted to authorized VA IT employees. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at the health care area, or an OIG office location remote from the health care area, is controlled in the same manner.

Access to the Area Puget Sound Information System working and storage areas is restricted to VA employees who must complete both the HIPAA and Information Security training. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information System Security r (ISSO), local Area Manager, System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

Human Resources notify Divisions, IT and ISSO of new hires and their start date(s), through email, and new accountrequests. The Division that the person is going into fills out the local access form, Automated Systems Access Request form, with name, SSN and/or claim number, job title, division and telephone number, along with marking the boxes on the form for application access the user will need on the computer system. This form starts at the Division level, is signed by the Division Chief, then goes to the ISSO and Director, for signatures and then to IT for implementation. Documentation is filed in an employee folder and maintained in the ISSO's office.

- Individuals are subject to a background investigation before given access to Veteran's information.
- All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually AND Privacy and HIPAA Focused Training.

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 forthese 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 theOffice of General Counsel.

8.2 Will VA contractors have access to the Area Boundary and the PII? If yes, what involvement willcontractors have withthe designand maintenance of the Area Boundary? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors whowork 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 will have access to the Area Puget Sound Information System after completing the VA Privacy and Information Security Awareness trainingand Rules of Behavior annually, and after the initiation of a background investigation. Contractors are only allowed access for the duration of the contract this is reviewedby the privacy officer and the designated Contracting Officer Representative (COR). Per the National Contractor Access Program (NCAP) guidelines, contractors can have access to the Area Puget Sound InformationSystem only after completing mandatory information security and privacy training, Privacy and HIPAA Focused Training as well as having completed a Special Agency Check, finger printing and having the appropriate background investigation scheduled with Office of Personnel Management. Certification that this training has been completed by all contractors must be provided to the employee who is responsible for the

contract in question. In addition, all contracts by which contractors might access sensitive patient informationmust include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy. Contractors with VA Area Puget Sound Information System access must have an approved computer access request on file. The area manager, or designee, in conjunction with thearea ISSO and the applicable COR reviews accounts for compliance with account management requirements. User accounts are reviewed periodically in accordance with National schedules.

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

VA offers privacy and security training. Each program or Area Boundary may offer training specific to the programor 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 Area Puget Sound Information System 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 andresponsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained.

The Talent Management System offers the followingapplicable 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 date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*
4. *The FIPS 199 classification of the Area Boundary (LOW/MODERATE/HIGH).*

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

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

The Area Puget Sound Information System underwent an OIG audit by the VA Certification Program Office (CPO) insupport of FISMA compliance, this was completed in July 09, 2017. The Area Puget Sound authorization date was May 2018. The FIPS 199 classification is moderate. The ATO is current through April 2021.

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

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

Signature of Responsible Officials

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

Privacy Officer Signature

Area PO's:	Signature:
James Weivoda	
Jeffery Swanberg	
Chiquita Charles	
Allison Conn	
Cesar Romero	

Information System Security Officer (ISSO) Signature

Area ISSO's:	Signature:
Yosief Fesseha	
Sharon Lepage-Erwin	
Gerry Ambalada	
Benjamin Krueger	

——————————————————————————

Area Manager Signature

Area Manager:	Signature:
Bruce Gibson	

The Area Manager below attests that the information provided in this Privacy Impact Assessment is true and accurate.

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

PII Mapped to Components Table

The below table is a full accounting of servers and databases aa of this date, at Area VA Puget Sound. With IT lack of ability to visibility audit the content of databases we have made some assumptions as to the content of the databases in the below table. Privacy, Records Management and Information Technology aye doing a 100% audit of all databases to validate the current owner, contents (PII/PHI), current need for the storage of the data, and records retention of the data.

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
Server OITPUGSQL001: • 3M_Clean-Trace • AccountTracking • AML10.6RightFax • Archive • ATSABS • ATSCOMPASS • Carol • Censis_Beta_V2_Global • censis_graphics • Censis_HL1317 • Censis_SG1317 • CensisBufferAgent • CentrakWPSAML • CentrakWPSPUG • cori_net • CoriHL7 • DEMODATA • DEMODATA_57H0NRS0C • EMR • Global • IT_Inventory • LAKE_Device_Registration • LAKE_Device_Registration_7.13 • Lake_OM_DB • lmi_area_monitor • Lynx • Maintenance • MaintenanceLog	Yes	Yes	Yes	Personal Identifiable Information (PII) Protected Health Information (PHI) Individually Information (III)	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	VAMC Puget Sound

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
Server VHAPUGSQL12: • AML_OM_3.2.27.57 • BOI • DeviceRegistration • ntisocial • POR • PORPolyTest • PUG • SmithsSolisC	Yes	Yes	Yes	Personal Identifiable Information (PII) Protected Health Information (PHI) Individually Information (III)	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	VAMC Puget Sound
Server VHAPUGSQL3 • WPDR_Development	Yes	Yes	Yes	Personal Identifiable Information (PII) Protected Health Information (PHI) Individually Information (III)	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	VAMC Puget Sound
Server VHAPUGSQL30\ARTSQLSERVER: • ART • ART_2002 • ART_2003 • ART_2004 • ART_2005 • ART_2006 • ART_2007 • ART_2008 • ART_2009 • ART_2010 • ART_2011 • ART_2012 • ART_2013 • ART_2014	Yes	Yes	Yes	Personal Identifiable Information (PII) Protected Health Information (PHI) Individually Information (III)	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	VAMC Puget Sound

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
• ART_2015 • ART_2016 • ART_Test • ReportServer • ReportServer$ARTSQLSERVER • ReportServer$ARTSQLSERVERTempDB • ReportServerTempDB							
Server VHAPUGSQL30\HSRDSQLSERVER: • BI_PM_CDW_Data • C3P • C3P1 • C3P2 • C3PStudy • Cambia_MIRB • CB • CDW_METADATA • CHOICE • CHOICE_CDW_Data • CommEOL • CommEOL2Archive • CommEOL3 • CommEOLValidation • CONCERT_COPD_Data_Hub_V1_C6 • CONCERT_COPD_Data_Hub_V3_C6 • CONCERT-CER-COPD • CONCERT-CER-UWBOISE-PFT • CONCERT-CER-UWCLN • CONCERT-CER-UWHV-SUBSET • CSP256_Dev • CSP256_ID • CSP569_Analysis • CSP569_Dev • CSP569_ID • CSP595_Respiratory_Health_MIRB • CSP992_Dev • CSP992_ID • CSP993_DEV • CSP993_ID • CSP997_Dev • CSP997_ID • Dominitz-IBD-MIRB • EOLUtilization • EPRP_COPD_Depression_Study	No	Yes	No	PII / PHI Research Data	Research Studies	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VAMC Puget Sound

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
• EPRP_COPD_Depression_Study_CDW_Pharmacy • ERIC_NVVLSR • ERIC_VHES_MIRB • HAIG_NATIONAL • HAIG_VISN_20 • HSRD_SDM_Evaluation_QI • IBD • ICU_HRQOL_Source • IHAMI • INCASE • INSIGHT_COPD • LOTT • LOTT_Crosswalk • LOTT_NatlScreen • MOVE_RRP • ONS_APRN_Evaluation_QI • OPH_Prevalence_of_Cirrhosis_QI • Optimizing_Value_By_Nurse_Practitioners_Source • Optimizing_Value_By_Nurse_Practitioners_Source_1 • Optimizing_Value_By_Nurse_Practitioners_Work • ORH_OVAC_EConsult_Best_Practices_QI • ORH_OVAC_Exp_Choice_Prv_Network_QI • PCO_ORH_VIMPACT_QI • QUERI_ICS_QI • QUERI_TripleAim • QUERI_TripleAim_Staging • SCEval_QI_RestrictedAccess • SCEval_QI_RestrictedAccess_NCPS • SCEval_QI_RestrictedAccess_Source • SCEval_QI_RestrictedAccess_Work • Surgical_Value_NSQIP_MIRB • TIDES_PTSD • TIU • TIU_Analysis • TIU_STAGING • TIU_TempWork • TIU_VISN20_Text • TIU_VISN20_Text_Temp • TumorRegistry • V20_ORH_COPD_REGISTRY • VinceFan2 • VirtualManagerDB • VISN20_DW_Migration_DM • VISN20_DW_Migration_DM_1							

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
• VISN20_DW_Migration_Hu_Temp1 • WAVES							
Server OITPUGSQL016: • Censis_Beta_V2_Global • censis_graphics • Censis_HL1317 • Censis_SG1317 • CensisBufferAgent	No	No	No	None	None	N/A	VAMC Puget Sound
Server OITPUGSQL001: • SystemState	No	No	No	None	None	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VAMC Puget Sound
Server VHAPUGSQL12: • SystemState	No	No	No	None	None	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VAMC Puget Sound
Server VHAPUGSQL3: • SystemState	No	No	No	None	None	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VAMC Puget Sound

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
Server VHAPUGSQL30\ARTSQLSERVER: • SystemState	No	No	No	None	None	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VAMC Puget Sound
Server R01V20APPRPL01 • ReportServer • ReportServerTempDB • SystemState	No	No	No	None	None	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VAMC Puget Sound
Server OITPUGSQL012: • SystemState	No	No	No	None	None	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VAMC Puget Sound
Server OITPUGSQL001: • AuditTrail • AWP • AWPSys • MATRIXCTRL • MATRIXCTRL_57H0NRS0C • MATRIXCTRL_57N0PLAS3 • MATRIXCTRL_57N0PSYLC • MATRIXCTRL_57O0Y0Y7X • MATRIXCTRL_57O16NUCT • MATRIXCTRL_57O16OIAL • MATRIXCTRL_57O18EMU7	No	No	No	None	None	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VAMC Puget Sound

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
• MATRIXCTRL_57P0IMP1K • MATRIXCTRL_5KL0XN46Z • MATRIXCTRL_5WJ0HXC0E • MATRIXCTRL_5WJ0HXZJS • MATRIXCTRL_5WP0XFWNS • MATRIXCTRL_5X10FXEA6 • MATRIXCTRL_5XJ0W2LK9 • MATRIXCTRL_5XP0PGAFD • MATRIXCTRL_5Y10XMU9H • MATRIXCTRL_5Y20WCO6B • MATRIXCTRL_5YH0Y3Y03 • MATRIXCTRL_5YI0ZBNBL • MATRIXCTRL_5YT0HPXDW • PUGKEYS • PUGKEYS_5WJ0HXC0E • PUGKEYS_5WP0XFWNS • PUGKEYS_5X10FXEA6 • PUGKEYS_5XJ0W2LK9 • PUGKEYS_5XP0PGAFD • PUGKEYS_5Y10XMU9H • PUGKEYS_5Y20WCO6B • PUGKEYS_5YH0Y3Y03 • PUGKEYS_5YI0ZBNBL • PUGKEYS_5YT0HPXDW • SEA_OM_DB • SEA10.6RightFax • SM20040 • SM20040_57N0PSYLC • SM20040_5KL0XN46Z • SM20040_5WJ0HXZJS • Tempmonitor • VISN20BIOML • WICMASTER							
Server OITPUGSQL001: • AuditTrail • AWP • AWPSys • MATRIXCTRL • MATRIXCTRL_57H0NRS0C • MATRIXCTRL_57N0PLAS3 • MATRIXCTRL_57N0PSYLC • MATRIXCTRL_57O0Y0Y7X • MATRIXCTRL_57O16NUCT	No	Yes	No	PII / PHI Research Data	Research Studies	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with	VAMC Puget Sound

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
• MATRIXCTRL_57O16OIAL • MATRIXCTRL_57O18EMU7 • MATRIXCTRL_57P0IMP1K • MATRIXCTRL_5KL0XN46Z • MATRIXCTRL_5WJ0HXC0E • MATRIXCTRL_5WJ0HXZJS • MATRIXCTRL_5WP0XFWNS • MATRIXCTRL_5X10FXEA6 • MATRIXCTRL_5XJ0W2LK9 • MATRIXCTRL_5XP0PGAFD • MATRIXCTRL_5Y10XMU9H • MATRIXCTRL_5Y20WCO6B • MATRIXCTRL_5YH0Y3Y03 • MATRIXCTRL_5YI0ZBNBL • MATRIXCTRL_5YT0HPXDW • MIRB2002_SE • MIRECC_Admin • MIRECC_ADRC • MIRECC_Agitation • MIRECC_BNGRef • MIRECC_CSF2 • MIRECC_CSP • MIRECC_CTE • MIRECC_Debby_Data • MIRECC_DebbySource • MIRECC_DLB • MIRECC_Familial • MIRECC_FrozenTissue • MIRECC_Gail • MIRECC_GailSource • MIRECC_GWVI • MIRECC_IndustryTrack • MIRECC_KAME • MIRECC_Lab_06_24_10 • MIRECC_LabInventory • MIRECC_LabResult • MIRECC_Libby • MIRECC_MDS • MIRECC_NACC • MIRECC_Neuropath_Data • MIRECC_NonADRC • MIRECC_NP • MIRECC_PoND • MIRECC_PoNDtwo						restricted access controls	

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
• MIRECC_PrazosinETOH • MIRECC_PrazosinPTSD • MIRECC_PREDICT • MIRECC_PTH • MIRECC_Rebekah • MIRECC_ReCOUP • MIRECC_Simvastatin • MIRECC_SIS • MIRECC_Source_data • MIRECC_SSISLOGGING • MIRECC_SSISTRAINING • MIRECC_TAIC • MIRECC_TBI • MIRECC_TBI_20191105 • MIRECC_TBI_Freeze_20180514 • MIRECC_TBI_Freeze_20190110 • MIRECC_TBI_Freeze_20190515 • MIRECC_TBI_Freeze_20200219 • MIRECC_TBI_Freeze_20201030 • MIRECC_TrackingLog • MIRECC_UDS_06_10_Data • MIRECC_Working • MIRECC_WPDR • OnTrack • pckits • PUGKEYS • PUGKEYS_5WJ0HXC0E • PUGKEYS_5WP0XFWNS • PUGKEYS_5X10FXEA6 • PUGKEYS_5XJ0W2LK9 • PUGKEYS_5XP0PGAFD • PUGKEYS_5Y10XMU9H • PUGKEYS_5Y20WCO6B • PUGKEYS_5YH0Y3Y03 • PUGKEYS_5YI0ZBNBL • PUGKEYS_5YT0HPXDW • Research • SEA_Device_Registration • SEA_DeviceRegistration7_13 • SEA_OM_DB • SEA10.6RightFax • SFFX • SFFXResearch • SM20040							

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
• SM20040_57N0PSYLC • SM20040_5KL0XN46Z • SM20040_5WJ0HXZJS • Tempmonitor • VAPugetSound							
Server VHAPUGSQL30\ARTSQLSERVER: • ART_2017 • ART_2018	Yes	Yes	Yes	Personal Identifiable Information (PII) Protected Health Information (PHI) Individually Information (III)	This data is needed for management business operations	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VAMC Puget Sound
Server VHAPUGSQL30\HSRDSQLSERVER: • ACHIEVE • Admin • Au_Portfolio_Administration • Colectica • Colectica-aspnet5-users • DELITE • DialysisTiming_Source • EMBRACE • HSRD_Data_Group • National_VETPRAMS • OMHO_Centralized_Caring_Letters • OPCCCT_EPCCVA • OVAC_VACE_VA_Access_Eval_QI • Provider_Network • RegerSDR • RELIEF • SCS_ORH_VA_ECHO_QI • Spark • Spark_Archive • Temp • Workforce	**No**	**No**	**No**	**PII / PHI Research Data**	**Research Studies**	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VAMC Puget Sound

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
Server OITPUGSQL012: • BIORAD_VAMC • ContinuumDB • iMed37 • iMedAudit • UpdateHistory • zzHL7 • zzNew • zzOld • zzPAT	**No**	**No**	**No**	**None**	**None**	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VAMC Puget Sound
Server OITPUGSQLRES001\HSRDSQLSERVER: • Admin • BI_PM_CDW_Data • CDW_METADATA • CSP595_SHADE • ERIC_FLAReS • FAN_PUMA_COPD • Gray_Together2Lose_MIRB • HSRD_SFFX_Completed_Incident_Tracking • JIRA • MOVE_UP_RCT • OCC_VACEATLAS • OMHSP_TMH2 • ORH_OVAC_EConsult_Best_Practices_QI • REMODEL_SLEEP • SCEval_QI_RestrictedAccess • SCEval_QI_RestrictedAccess_Source • SystemState • TEST1	**No**	**Yes**	**No**	**PII / PHI Research Data**	**Research Studies**	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VAMC Puget Sound
Server OITPUGSQLRES001\ARTSQLSERVER: • ART • ART_2015 • ART_2016 • ART_2017 • ART_2018 • ART_2019 • ART_Test • ReportServer$ARTSQLSERVER • ReportServer$ARTSQLSERVERTempDB • SystemState	Yes	Yes	Yes	Personal Identifiable Information (PII) Protected Health Information (PHI) Individually	This data is needed for management business operations	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VAMC Puget Sound

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
				Information (III)			
Server PUG-LT-144908\SQLEXPRESS: • None	No	No	No	None	None	N/A	VAMC Puget Sound
Server OITPUGSQL016: • ApplicationModules • Cochlear • ION_Data • ION_Network • ION_SystemLog • Maestro • NOAHDatabaseCore • NuanceMC • SEA_ASAudit • SEA_DRS_7.13 • SEA_OM_4.0 • SilhouetteCentral • Soundwave • SystemState • Tempmonitor • Viewpoint • VOPRO_Configuration_Production • VOPRO_Document_Production • VOPRO_Logs_Production	No	No	No	None	None	N/A	VAMC Puget Sound
Server OITPUGSQL016\VBA: • SystemState	No	No	No	None	None	N/A	VARO Puget Sound
Server VHAPUGAPPKW\KWTTSERVER14: • None	No	No	No	None	None	N/A	VAMC Puget Sound
Server PUG-WS-162583: • None	Yes	No	No	None	None	N/A	VAMC Puget Sound