



Date PIA submitted for review:

12/14/2023

Privacy Impact Assessment for the VA Area called¹:

AREA SPOKANE-WALLA WALLA DISTRICT 5 – PACIFIC

¹ The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, 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.

Sites within Area:

<i>Sites</i>	<i>Station Numbers</i>
1) V20/668 Spokane, WA HCS	668
a) Mann-Grandstaff VA Medical Center (VAMC)	668
b) Bonner County Clinic (RHCC)	668GD
c) Coeur d’Alene Community-Based Outreach Clinic (CBOC)	668GB
d) Health Care for Homeless Vets	668QE
e) Libby Rural Health Care Clinic (RHCC)	668QB
f) Mayfair Bldg.	668
g) North Wall Street Bldg.	668
h) Spokane Valley Vets Center	668GC
i) Wenatchee CBOC	668GA
j) WSU Clinic	668QE
2) V20/687 Walla Walla, WA HCS	687
a) Johnathan M. Wainwright Memorial VAMC	687
b) Boardman Primary Care Telehealth Outreach Clinic (PCTOC)	
c) Enterprise PCTOC	
d) La Grande CBOC	687GC
e) Lewiston CBOC	687GB
f) Richland CBOC	687GA
g) Walla Walla Vets Center	
h) Yakima Valley CBOC	687HA
i) Yakima Vets Center	

Area Contacts:

Area Key Stakeholders

<i>Name</i>	<i>Title (PO, ISSO, AM, MD/SPS Staff, Facility Director)</i>	<i>Phone Number</i>	<i>Email Address</i>	<i>Applicable Site (VBA, VHA, NCA, Program Office)</i>
Nicholas Quinn	Privacy Officer	(509) 434-7525	nicholas.quinn2@va.gov	VHA
Harvey H. Howell	Privacy Officer	(509) 525-5200 x26428	Harvey.howell@va.gov	VHA
Douglas K. Bell	Information System Security Officer	(509) 434-7467	Douglas.bell4@va.gov	VHA

<i>Name</i>	<i>Title (PO, ISSO, AM, MD/SPS Staff, Facility Director)</i>	<i>Phone Number</i>	<i>Email Address</i>	<i>Applicable Site (VBA, VHA, NCA, Program Office)</i>
Joseph Hoffman	Information System Security Officer	(509) 910-4595	joseph.hoffman3@va.gov	VHA
Scott Brown	Area Manager	(509) 434-7430	scott.brown8@va.gov	VHA

Abstract

The abstract provides the simplest explanation for “what does the Area do?”.

Area Spokane-Walla Walla is an Information Area that consists of Mann-Grandstaff Veteran Affairs Medical Center (VAMC), Johnathan M. Wainwright Memorial (VAMC), Coeur d’Alene Community Based Outpatient Clinic (CBOC), Wenatchee Community Based Outpatient Clinic (CBOC), La Grande Community Based Outpatient Clinic (CBOC), Lewiston Community Based Outpatient Clinic (CBOC), Richland Community Based Outpatient Clinic (CBOC), North Wall Street Building., Health Care for Homeless Vets, Libby Rural Health Clinic (RHC), Mayfair Building, Washington State University (WSU) Clinic, Bonner County Rural Health Clinic (RHC), Boardman (PCTOC), Enterprise (PCTOC), Spokane Valley Vets Center, Walla Walla Vets Center, Yakima (CBOC), and Yakima Vets Center. The Area 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 at data centers, and connectivity to other systems. Network connectivity rules are enforced by VA approved baselines for router and switch configurations. The Area system environment also includes as applicable, subsystem storage utilities such as tape drives, optical drives, disk drives, network attached storage (NAS), storage area networks (SAN), archival appliances, special purpose systems, and tier 2 storage solutions. The Area 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 employs a myriad of routers and switches that connect to the VA network.

Special Purpose Systems are non-medical, non-research VA network-connected, and non-Office of Information and Technology (OIT) supported Operational Technology (OT) device/system that cannot obtain a VA approved baseline.

Overview

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

- *The Area name and the name of the sites within it.*
- *The business purpose of the Area and how it relates to the program office and agency mission.*
- *Whether the Area is leveraging or accessing Enterprise repositories such as Veterans Benefits Management System, SharePoint, VistA, etc. and if so, a description of what PII/PHI from the Enterprise repositories is being used by the facilities in the Area.*
- *Documentation of any repository not maintained at the enterprise level, unlike Veterans Benefits Management System, SharePoint, VistA, etc. used by the facilities to collect, use, disseminate, maintain, or create PII/PHI.*
- *Any external information sharing conducted by the facilities within the Area.*
- *A citation of the legal authority to operate the Area.*
- *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 host or maintain cloud technology? If so, does the Area have a FedRAMP provisional or agency authorization?*

The Area Spokane-Walla Walla itself does not collect, use, disseminate, maintain, or store PII/PHI. VHA, VBA and NCA Facilities located within the Spokane-Walla Walla IT Area all access VA Enterprise IT systems respectively, hosted and maintained outside of this Area. These are VISTA, Veterans Benefits Management System (VBMS), Memorial Benefits System (MEM), etc.

Special Purpose Systems consists of specialized devices, and applicable components, hosted within the facilities associated to the Area. The system environment is comprised of operational technology devices/systems that assist, support, and maintain mission capabilities and operations for building safety, healthcare services, security services and other general services functional support areas.

The system environment may include, but are not limited to; energy management systems, heating ventilation and air conditioning (HVAC), temperature controls, building/facility access controls, building automation systems, utility control systems, distributed control systems, security cameras, emergency response vehicle dashcams, Virtual Reality (VR) headsets, promethean boards, TUG robots, Telesitter, and other business Operational Technologies. All Special Purpose Systems are identified in **Appendix C**.

Only PII/PHI collected and used by the facilities within the Area will be referenced in this document since the Area does not maintain, disseminate, or store information accessed by each facility.

The facilities within the Area collect, use, and/or disseminate PII/PHI that is maintained and stored within enterprise systems such as VistA, Veterans Benefits Management System (VBMS), Burial Operations Support System (BOSS)/ Automated Monument Application System (AMASS), etc. There are [individual PIAs](#) that contain detailed information on the maintenance, dissemination and sharing practices, and storage of the PII/PHI for each Enterprise system accessed by the facilities.

The Area is using the VA Enterprise Cloud (VAEC) which is at the enterprise level and is outside of the Area. Further information can be found in the VAEC PIA.

The applicable [SORs](#) for Area Spokane-Walla Walla include:

Site Type: VBA/VHA/NCA or Program Office	Applicable System of Records (SORs)
*VHA	<ul style="list-style-type: none"> • Non-VA Fee Basis Records-VA, SOR 23VA10NB3 • Patient Medical Records-VA, SOR 24VA10A7 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA10 • 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 79VA10 • Income Verification Records-VA, SOR 89VA10NB • Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA13 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10 • National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147VA10NF1 • VHA Corporate Data Warehouse- VA 172VA10A7 • Health Information Exchange - VA 168VA005 • Applicants for Employment under Title 38, USC-VA, SOR 02VA135 • Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attendings, and Others, or Paid Indirectly through a Disbursement Agreement) Personnel Records- VA, SOR 14VA05135 • Non-VA Fee Basis Records- VA, SOR 23VA163 • Patient Medical Records- VA, SOR 24VA19 • Health Care provider Credentialing and Privileging Records- VA, SOR 77VA10Q • Income Verification Records- VA, SOR 89VA19 • Telephone Service for Clinical Care Records- VA, SOR 113VA112 • The Revenue Program Billings and Collection Records- VA, SOR 114VA16 • National Patient Databases- VA, SOR 121VA19
Special Purpose Systems	<ul style="list-style-type: none"> • Applicants for Employment Under Title 38 – VA SOR 02VA135 • Employee Medical File System Records – VA SOR 08VA05 • Patient Advocate Tracking System Replacement (PATS-R) – VA SOR 100VA10H • Police and Security Records – VA SOR 103VA07B • Compliance Records, Response, and Resolution of Reports of Persons Allegedly Involved in Compliance Violations – VA SOR 106VA17 • Enrollment and Eligibility Records – VA SOR 147VA10 • Non-VA Care (Fee) Records – VA SOR 23VA10NB3 • Patient Medical Records – VA SOR 24VA10A7

Site Type: VBA/VHA/NCA or Program Office	Applicable System of Records (SORs)
	<ul style="list-style-type: none"> • Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA SOR 54VA10NB3 • Community Placement Program – VA SOR 65VA122 • Health Care Provider Credentialing and Privileging Records – VA SOR 77VA10A4 • Veterans Health Information Systems and Technology Architecture (VistA) Records – VA SOR 79VA10 • Automated Safety Incident Surveillance and Tracking System – VA SOR 99VA13 • HealthShare Referral Manager (HSRM) – VA SOR 180VA10D • Community Care (CC) Provider Profile Management System (PPMS) – VA SOR 186VA10D

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, or technology being developed.

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

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

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

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 collects. If additional PII/PHI is collected, please list those in the text box below:

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> Name | <input checked="" type="checkbox"/> Emergency Contact | <input checked="" type="checkbox"/> Vehicle License Plate |
| <input checked="" type="checkbox"/> Social Security | <input checked="" type="checkbox"/> Information (Name, Phone | <input checked="" type="checkbox"/> Number |
| <input checked="" type="checkbox"/> Number | <input checked="" type="checkbox"/> Number, etc. of a different | <input checked="" type="checkbox"/> Internet Protocol (IP) |
| <input checked="" type="checkbox"/> Date of Birth | <input checked="" type="checkbox"/> individual) | <input checked="" type="checkbox"/> Address Numbers |
| <input checked="" type="checkbox"/> Mother's Maiden Name | <input checked="" type="checkbox"/> Financial Account | <input checked="" type="checkbox"/> Current Medications |
| <input checked="" type="checkbox"/> Personal Mailing | <input checked="" type="checkbox"/> Information | <input checked="" type="checkbox"/> Previous Medical |
| <input checked="" type="checkbox"/> Address | <input checked="" type="checkbox"/> Health Insurance | <input checked="" type="checkbox"/> Records |
| <input checked="" type="checkbox"/> Personal Phone | <input checked="" type="checkbox"/> Beneficiary Numbers | <input checked="" type="checkbox"/> Race/Ethnicity |
| <input checked="" type="checkbox"/> Number(s) | <input checked="" type="checkbox"/> Account numbers | <input checked="" type="checkbox"/> Tax Identification |
| <input checked="" type="checkbox"/> Personal Fax Number | <input checked="" type="checkbox"/> Certificate/License | <input checked="" type="checkbox"/> Number |
| <input checked="" type="checkbox"/> Personal Email | <input checked="" type="checkbox"/> numbers | |
| <input checked="" type="checkbox"/> Address | | |

- | | | |
|--|--|--|
| <input checked="" type="checkbox"/> Medical Record Number | <input checked="" type="checkbox"/> Service-connected Disabilities | <input checked="" type="checkbox"/> Education Information |
| <input checked="" type="checkbox"/> Next of Kin | <input checked="" type="checkbox"/> Employment Information | <input checked="" type="checkbox"/> Gender |
| <input checked="" type="checkbox"/> Guardian Information | <input checked="" type="checkbox"/> Veteran Dependent Information | <input checked="" type="checkbox"/> Tumor PHI Statistics |
| <input checked="" type="checkbox"/> Electronic Protected Health Information (ePHI) | <input checked="" type="checkbox"/> Disclosure Requestor Information | <input type="checkbox"/> Other Unique Identifying Information (list below) |
| <input checked="" type="checkbox"/> Military History/Service Connection | <input checked="" type="checkbox"/> Death Certification Information | |
| | <input checked="" type="checkbox"/> Criminal Background | |

PII Mapping of Components (Servers/Database)

Area Spokane-Walla Walla consists of 89 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 Spokane-Walla Walla and the reasons for the collection of the PII are in the **Mapping of Components Table in [Appendix B](#) of this PIA.**

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

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 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 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 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, and 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.

The information that resides within the facilities in the Area 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.

Depending on the type of information, it may also come from the Veterans Benefits Administration (VBA), the VA Health Eligibility Center (HEC), VA Network Authorization Office (NAO) for non-VA Care payments, and non-VA medical providers, Department of Defense (DOD), Internal Revenue Service (IRS), Office of Personnel Management (OPM), Social Security Administration (SSA), Federal Emergency Management Agency (FEMA), Federal Bureau of Investigation (FBI).

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.

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, or created by the Area itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

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

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

Means of Collection Table

Site Type: VBA/VHA/NCA or Program Office	Means of Collection
*VHA	Information collected directly from patients, employees and/or other members of the public is collected using paper forms (such as the VA Form 10-10EZ enrollment form for VA health care), or interviews and assessments with the individual. Much of the information provided by veterans or other members of the public, such as address and phone number, next of kin and emergency contact information, and similar information are assumed to be accurate because it is provided directly by the individual. Additionally, information entered into an individual's medical record by a doctor or other medical staff is also assumed to be accurate.

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 Spokane-Walla Walla using several methods, including verbally from Veterans, caregivers, legal guardians, paper documents, facsimiles, and electronically from the community and/or federal agencies. 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).

These data collections may be done using secure web portals, VPN connection, e-mail, and facsimile.

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 is necessary to the program’s or agency’s mission. Merely stating the general purpose of the Area without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

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

The purposes of the information from Veterans and other members of the public collected, maintained, and processed by Area Spokane-Walla Walla are as varied as the types of information collected.

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

Purpose of Information Collection Table

Site Type: VBA/VHA/NCA or Program Office	Purpose of Information Collection
*VHA	<ul style="list-style-type: none"> • To determine eligibility for health care and continuity of care • Emergency contact information in 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

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

Discuss whether and how often information stored in a facility within the Area 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 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 checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

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

Information that is collected and used directly from enterprise systems have additional details regarding checks for accuracy 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 accurate because 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 service history 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 obtained directly 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, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.

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

Site Type: VBA/VHA/NCA or Program Office	Legal Authority
*VHA	<ul style="list-style-type: none"> • Veterans 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.

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 Spokane-Walla Walla 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:

VA Area Spokane-Walla Walla 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 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 MyHealthVet 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.
- **Vehicle License Plate Number:** Used for assignment of employee parking and assignment of parking during events
- **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.
- **Tax Identification Number:** Used for employment, eligibility verification
- **Medical Record Number:** Used to identify a patient within the medical record system without using their social security number as their identifier.
- **Next of Kin:** Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
- **Guardian Information:** Used when patient is unable to make decisions for themselves.
- **Electronic Protected Health Information (ePHI):** Used for history of health care treatment, during treatment and plan of treatment when necessary.
- **Military history/service connection:** Used to evaluate medical conditions that could be related to location of military time served. It is also used to determine VA benefit and health care eligibility.
- **Service-connected disabilities:** Used to determine VA health care eligibility and treatment plans/programs
- **Employment information:** Used to determine VA employment eligibility and for veteran contact, financial verification.
- **Veteran dependent information:** Used to determine benefit support and as an emergency contact person.
- **Disclosure requestor information:** Used to track and account for patient medical records released to requestors.
- **Death certificate information:** Used to determine date, location and cause of death.

- **Criminal background information:** Used to determine employment eligibility and during VA Police investigations.
- **Education Information:** Used for demographic background information for patients and as a determining factor for VA employment in areas of expertise. Basic educational background, e.g. High School Diploma, college degree credentials
- **Gender:** Used as patient demographic, identity and indicator for type of medical care/provider and medical tests required for individual.
- **Tumor PII/PHI Statistics:** Used to evaluate medical conditions and determine treatment plan
- **Date of Death:** Used to verify spousal and beneficiary relationship to Veteran, at time of death
- **Marital Status:** Used to verify spousal and beneficiary eligibility
- **Service Information:** Used to verify eligibility
- **Benefit Information:** Used to verify burial benefits
- **Relationship to Veteran:** Used to determine relationship to Veteran
- **Funeral Home Information:** Used to contact funeral home or other service coordinator information

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

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

Many facilities within an Area 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 conduct and the data that is created from the analysis.

If the facility creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly

created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

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

The VA Area Spokane-Walla Walla uses statistics and analysis to create general reports that provide the VA a better understanding of the delivery of patient care, patient satisfaction, etc. 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, fee services, etc.
- Daily bed management activity
- Coding averages for outpatient/inpatient encounters
- Satisfaction of Healthcare Experience of Patients (SHEP) data as it pertains to customer satisfaction regarding outpatient/inpatient services
- Unique patient trends
- Clinic wait times

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

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

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

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

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

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

The controls in place to assure 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?

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

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

The Area Spokane-Walla Walla itself, does not 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
- Tax Identification Number
- Medical Record Number
- Vehicle License Plate Numbers
- Service Information
- Benefit Information
- Relationship to Veteran
- Funeral Home Information
- Name and address of Next of Kin
- Military service data, applicant’s name and address, place of burial, burial service, and headstone data.

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

Length of Retention Table

Site Type: VBA/VHA/NCA or Program Office	Length of Retention
*VHA	<ul style="list-style-type: none"> • 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.

Site Type: VBA/VHA/NCA or Program Office	Length of Retention
	<p>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</p> <ul style="list-style-type: none"> 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.

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 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

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 Spokane-Walla Walla is destroyed by the disposition guidance of RCS 10-1. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014)

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.

3.5 Does the Area 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

The Area Spokane-Walla Walla does not incorporate research or testing programs; however, the Mann-Grandstaff VA Medical Center is a training facility for the Valor Nurses program, nursing students, phlebotomy students, dental students, dental residents, medical students/residents, etc. PII/PHI is not incorporated in any training material and resides only in the test and production environments within the Area network.

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.

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by Area Spokane-Walla Walla could be retained for longer than is necessary to fulfill the VA mission. Records held longer than

required are at greater risk of being unintentionally released, 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 Spokane-Walla Walla 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 Spokane-Walla Walla ensures that all personnel involved with the collection, use and retention of data are 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 from the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning the proper handling of 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.

4.1 With which internal organizations are facilities within the Area sharing/receiving/transmitting information with? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Note: Question #3.5 (second table) in the Area Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

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

List the Program Office or IT System information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT System	List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT System	Describe the method of transmittal	Applicable Sites within Area (VBA, VHA, NCA, Program Office)
Veterans Benefits Administration (VBA)	Filing benefit claims	Social Security Number, Benefits Information, ClaimsDecision, DD-214, PertinentPersonally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) appropriate to the request	Compensation and Pension Record Interchange (CAPRI) electronic software package	Spokane Walla Walla (all sites within the area)
Veterans Health Administration (VistA)	Electronic Health Record	Area Log files, sample clinical data that may contain Protected Health Information (PHI)	Electronically pulled from VistA thru Computerized Patient Record Area (CPRS)	Spokane Walla Walla (all sites within the area)
Veteran’s Health Information Exchange (VHIE) a.k.a. Virtual Lifetime Electronic Record (VLER)	Electronic Health Record	Patient demographic information (e.g., name, address, phone numbers, date of birth, social security number, internal control number); patient demographic and health information from external health care providers (e.g., medication listing allergies, consultations and referrals, progress notes, history and physicals, and procedure notes, Advanced Directives, problem lists, laboratory reports, lists of procedures and encounters); benefits information (e.g., disability rating, service	Secure web portal VLER/NwHIN partners and the Department of Defense via the VHIE secure portal/adaptor.	Spokane Walla Walla (all sites within the area)

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT System</i>	<i>Describe the method of transmittal</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
		connection rating); and information on Veterans' preferences for restricting the sharing of their health information (e.g., authorizations, restriction requests, revocation of authorizations); discharge summaries, diagnostic studies.		
Department of Veterans Affairs General Counsel Office	Electronic Health Record	Pertinent PII, PHI, and III appropriate to the request.	Transmitted upon request in an electronic, written, or verbal format based on the individual request.	Spokane Walla Walla (all sites within the area)
Department of Veterans Affairs Regional Counsel Office	Electronic Health Record	Pertinent PII, PHI, and III appropriate to the request.	Transmitted upon request, usually in electronic format.	Spokane Walla Walla (all sites within the area)
VA Network Authorization Office – Non- VA care payments	Electronic Health Record	Demographics, diagnoses, medical history, service connection, provider orders. VHA recommendation/approval for non-VA care.	Fee Basis Claim System (FBCS) authorization software program.	Spokane Walla Walla (all sites within the area)
VA Health Eligibility Center (HEC)	Eligibility	Service dates, SSN, demographics, service connection	Scanned documents uploaded into shared software programs	Spokane Walla Walla (all sites within the area)
West Consolidated WCPAC	Electronic Health Record	Diagnosis, service connection, dates of service	Electronically pulled from GSS	Spokane Walla Walla (all sites within the area)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The internal sharing of data is necessary individuals to receive benefits at the Area Spokane-Walla Walla. 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 unintended parties or recipients.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security 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 the facilities. 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 VA persons 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: Question #3.6 in the Area Privacy Threshold Analysis should be used to answer this question.

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

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

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a

Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT System	List the specific data element types such as PII/PHI that are shared/received with the Program or IT System	List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data	Applicable Sites within Area (VBA, VHA, NCA, Program Office)
Agfa HealthCare Corporation	The purpose of this agreement section is to establish a management agreement between VA and Agfa regarding the development, management, operation, and security of a connection between Agfa-supplied systems (i.e., PACS Systems (IMPAX), enterprise scheduling, (IMPAX Scheduling), Cardiovascular Information's Systems (CVIS),	For purposes of system troubleshooting, access to the Agfa Supplied Systems is provided though Agfa's Secure Remote Service System (SRSS) to review log files and sample clinical data from VA sites which may contain HIPAA Protected Health Information (PHI). This data is	HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R.) Part 164, Standards for Privacy of Individually Identifiable Health Information Privacy Act of 1974, 5 U.S.C. § 552a, as amended Patient Medical Record- VA 24VA10p2, Routine use #29 VA Claims Confidentiality Statute, 38 U.S.C § 5701	Site to Site VPN FIPS Compliant Transmission Standards.	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	reporting systems (TalkStation), Agfa's Enterprise Imaging Platform components, and third-party solutions sold by Agfa (e.g., PACS Health radiation dose tracking, TeraRecon advanced visualization, and Change Healthcare's QICS) and diagnostic imaging systems (computed radiology (CR) and digital radiology (DR)), owned by VA, and Agfa HealthCare's Secure Remote Service System (SRSS), owned by Agfa.	handled in accordance with Agfa's Business Associate Agreement (BAA) with the VA. Data Flow Description: In this case the PHI is not transmitted, collected, or stored. No information is moved from the Agfa-provided VA systems.			

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
Bayer HealthCare LLC	The purpose of this agreement section is to establish a management agreement between the VA and Bayer HealthCare LLC regarding the development, management, operation, and security of a connection between Bayer-provided software and contrast injection solutions, owned by VA, and the Bayer network, owned by Bayer.	Data sent or retrieved by Bayer may include diagnostic data, error messages, service status and Bayer software (Support Data). Data retrieved by Bayer may also include log files and DICOM files containing protected health information (VA PHI).	HIPAA Privacy Rule, 45 C.F.R. Part 164, Standards for Privacy of Individually Identifiable Health Information E-713 Privacy Act of 1974, 5 U.S.C. § 552a, as amended – Patient Medical Record – VA, 24VA10A7 Routine Use #29 VA Claims Confidentiality Statute, 38 U.S.C § 5701 (e)	Site to Site VPN, FIPS Compliant Transmission standards.	Area Spokane-Walla Walla
Deloitte Consulting Limited Liability Partnership	The purpose of this agreement section is to establish a management agreement between VA OIS and	Data collected includes network traffic metadata (e.g. origin IP address, destination IP	Federal Information Security Management Act (FISMA) VA Directive 6500, Managing Information Security Risk: VA	VPN Tunnel, TCP 3002,9092	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	<p>Deloitte regarding the development, management, operation, and security of a secured interconnection between the VA Network and Security Operations Center (NSOC) interconnection device(s) and the Deloitte’s interconnection device(s) listed under section 2.1 of this document. This interconnection will allow data to be securely transmitted from the Deloitte sensors deployed within VA’s enterprise network to Deloitte’s MSE secured enclave within Deloitte’s GPS TC.</p>	<p>address, time, connection state, port, protocol, user agent, bytes). The IP addresses are not directly traceable to the individual assigned to the IP address. Deloitte passively collects information and does not have the ability to manipulate network traffic or to modify VA’s in-place network security controls. No Personally Identifiable Information (PII), Protected Health Information (PHI), or VA sensitive</p>	<p>Information Security Program, and Handbook 6500, Risk Management Framework for VA Information Systems: Tier 3 – VA Information Security Program Cybersecurity Policy Compliance Analytics Support (CSPCAS) program (Task Order: VA118-17- F-2286; Contract: HHSN3162012000 18W) Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, Security Guide for Interconnecting Information Technology Systems Office of Management and</p>		

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
		information is expected to be transmitted by VA or received and stored by Deloitte. VA shall not provide PII, PHI, or VA sensitive information without providing advanced written notice to Deloitte.	Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Systems		
Draeger Medical, Inc.	The purpose of this agreement section is to establish a management agreement between VA and Draeger regarding the development, management, operation, and security of a connection between Draeger Innovian ARK System (ARK System) and Infinity	Draeger Service personnel have limited exposure to Protected Health Information (PHI) during the course of their duties through a view of Infinity Gateway Suite at VA servers. No actual PHI is transmitted. No data is	Privacy Act of 1974, 5 U.S.C. § 552a; 24VA10P2-Patient Medical Record VA. Routine Use 29. VA Claims Confidentiality Statute, 38 U.S.C § 5701 HIPAA Privacy Rule, 45 C.F.R. Part 164	Site to Site VPN Tunnel	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	Gateway Suite Software (Infinity Gateway) owned by VA, and the Draeger ServiceConnect® Remote Data Connection (RDC), owned by Draeger.	transmitted, only the remote connection is necessary for support. In the cases where logs files may be needed, we will work with an internal VA resource to obtain them. The PHI data stored behind the VA firewall on the Innovian system is as follows: Patient name, SSN, Healthcare Summary, Vital Signs, Lab Values, Heart Rate, Respiration,			
(VBMS) Experian Information Solutions Inc.	The purpose of this agreement section is to establish a management agreement between Department of	Information Type Transmitted: VA submits its debtor information files to Experian	HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R.) Part 164, Standards for Privacy of Individually Identifiable Health	Site to Site VPN Tunnel	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	VA and Experian Information Solutions Inc. regarding the development, management, operation, and security of a connection between VA CAO, owned by Department of VA, and Experian STS, owned by Experian Information Solutions Inc.	Information Solutions Inc. for the purpose of supplementing the data provided by other participating federal agencies into credit reporting systems. The submitted data will be surveyed for the purpose of determining whether an applicant has any delinquent federal debt. The transmitted data contains financial information and Personal Identification Information (PII) that includes Veterans' name, Social	Information <ul style="list-style-type: none"> • Privacy Act of 1974, 5 U.S.C. § 552a, as amended • VA Claims Confidentiality Statute, 38 U.S.C § 5701 • Confidentiality of Certain Medical Records, 38 U.S.C. § 7332 		

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
		Security Number (SSN), address, phone number, date of birth, and the individual amount of debt.			
GE Healthcare	The purpose of this agreement section is to establish a management agreement between VA and GE Healthcare regarding the development, management, operation, and security of a connection between GE Healthcare Systems, owned by VA, and GE Healthcare Online Center, owned by GE Healthcare.	Information Type Transmitted: GE currently utilizes the connection for providing software configuration changes and updates, maintenance, and troubleshooting of the GE Healthcare systems, so updates are transmitted on an as-needed basis. Other data traversing the connection include system	Privacy Act of 1974, 5 U.S.C. § 552a, Patient Medical Record-VA 24VA 10P2; Routine Use #29 VA Claims Confidentiality Statute, 38 U.S.C § 5701 HIPAA Privacy Rule, 45 C.F.R. Part 164 Confidentiality of Certain Medical Records, 38 U.S.C. § 7332 Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. § 5705 Freedom of Information Act (FOIA), 5 U.S.C. § 552	Site to Site VPN Tunnel	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
		<p>performance data and clinical information (both anonymized & identifiable). Data Flow Description: A remote operator employed by GE Healthcare will initiate an interconnection to GE Healthcare Online Center on VA network for technical and clinical application remote support using iLinq</p>			
<p>Olympus America Inc. (Olympus)</p>	<p>The purpose of this agreement is to establish a management agreement between VA and Olympus regarding the development,</p>	<p>Remote Desktop Sharing / Control, Preemptive support of Endoworks Server by monitoring</p>	<p>Privacy Act of 1974, 5 USC 552A, HIPPA Privacy Rule, 45 CFR Part 164, Confidentiality of Certain Medical Records, 38 USC 7332</p>	<p>Site to Site</p>	<p>Area Spokane-Walla Walla</p>

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	management, operation, and security of a connection between Olympus Products system owned by VA, and RSS.	basic system health, file transfer when necessary for troubleshooting, Top options for RSS connection, Site to Site VPN, CA Technology IT Client Automation 12.8, CA Technology Spectrum 9.2.3 (CA Technology SystemEdge 5.8)			
Omnicell, Inc	The purpose of this agreement section is to establish a management agreement between VA and Omnicell regarding the development, management, operation, and security of a connection between OmniCenter or WorkFlowRx	No Protected Health Information (PHI) data is transmitted from VA using the vSuite IDM solution. The VA controls how Omnicell gains access via the vSuite device software that has settings to enable/disable	HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R.) Part 164, Standards for Privacy of Individually Identifiable Health Information Privacy Act of 1974, 5 U.S.C. § 552a, as amended System of Record Notice, 24VA10p2, Patient Medical Record - VA, Routine Use #29.	Site to Site VPN Tunnel	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	or IVX or Pandora Server, owned by VA, and vSuite IDM solution, owned by Omnicell.	the https tunnel and/or appservices. This is set per device. There is a system tray icon where a user can see a notice when someone connects and click it to run an immediate audit report	VA Claims of Confidentiality 38 U.S.C. § 5701		
U.S. Office of Personnel Management Federal Investigative Services	OPM FIS is committed to utilizing technological tools in order to expedite elements of background investigations conducted on individuals (employees or applicants) for Federal employment, consultants, volunteers and/or contractor personnel, for national security	All Data Elements in Federal Forms SF85, SF 85P, and SF 86. Full Name, Date of Birth, Place of Birth, SSN, Other Names Used, Height, Weight, Hair Color, Eye Color, Sex, Phone Numbers, Name email and phone number of personal contacts, Passport	Executive Order (EO) 10450, Security Requirements for Government Employees, EO 12968, Access to Classified Information, EO 13467, Reforming Processes Relate to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information,	Secure Web Portal, Secure Socket Layer, FISMA Compliant Standards.	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	purposes, and for the purpose of satisfying the requirements of Homeland Security Presidential Directive 12 (HSPD-12)	Information, Citizenship Information, Current and previous addresses, Education History, Employment and Unemployment Records, Selective Service Record, Military History, Police Record, Drug Use and Drug Activity, Previous Investigations and Clearance Records, Financial Record, Association Records, and Finger Prints.	HSPD-12, Clinger-Cohen Act of 1996, Government Paperwork Elimination Act of 1998, e-Government Act of 2002, Intelligence Reform and Terrorism Prevention Act of 2004, The Atomic Energy Act of 1954 as amended.		
Parata Systems, LLC	The purpose of this agreement section is to establish a management agreement between VA	Information Type Transmitted: No sensitive data is transmitted between the	Privacy Act of 1974, 5 U.S.C. § 552a; System of Records; 24VA10P2; Patient Medical Record-VA; Routine Use	Site to Site	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	and Parata Systems, LLC regarding the development, management, operation, and security of a connection between Pharmacy Robotic Dispensing System, owned by VA, and Parata Technical Assistance Center, owned by Parata Systems, LLC.	VA and the Parata Systems, LLC. Data Flow Description: Data transmitted between the Parata Systems, LLC on the VA network is all relevant patient information required to process prescriptions to include: Patient Name, Address, Phone number, Social Security Number (SSN), Date of Birth, and prescription number.	#29. Confidential Nature of Claims, 38 U.S.C § 5701 HIPAA Privacy Rule, 45 C.F.R. Part 164		
Philips Healthcare, a division of Philips North America LLC	The purpose of this agreement section is to establish a management agreement	Information Type Transmitted: System Performance Parameters /	HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R.) Part 164, Standards for Privacy of	Site to Site VPN Tunnel	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	<p>between VA and Philips Healthcare regarding the development, management, operation, and security of a connection between the Philips Medical Devices, the Philips Vue Products and the Philips IntelliSpace PACS Radiology System, owned/leased by VA, and Philips RSN, SRSA System and CARE, owned by Philips Healthcare.</p>	<p>System Monitoring information, which may include but are not limited to the following: disk usage, reconstruction speed, image quality parameters, helium levels, temperature, humidity, and system error code information, acquisition parameter settings, system maintenance information i.e. scan time, kV, mA, X-ray tube heat. Patient images are also transmitted for image artifact troubleshooting,</p>	<p>Individually Identifiable Health Information Privacy Act of 1974, 5 U.S.C. § 552a, as amended, System of Record Notice, Patient Medical Record- VA 24VA10A7; Routine Use #29 VA Claims Confidentiality Statute, 38 U.S.C § 5701</p>		

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
		<p>which may include patient demographic data or Personal Identification Information (PII). Philips Healthcare will scrub data for any PII before assessments and before the data goes into the log files. The files are then purged.</p> <p>Data Flow Description: IPsec site-to-site VPN tunnel to establish a secure connection for services provided by RSN to remotely diagnose, repair, monitor and update various VA</p>			

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
		networked medical devices and clinical information systems.			
Philips Healthcare, a division of Philips North America LLC (CareStream)	The purpose of this agreement section is to establish a management agreement between VA and Philips Healthcare regarding the development, management, operation, and security of a connection between the Philips Medical Devices, the Philips Vue Products and the Philips IntelliSpace PACS Radiology System, owned/leased by VA, and Philips RSN, SRSA System and CARE,	Information Type Transmitted: System Performance Parameters / System Monitoring information, which may include but are not limited to the following: disk usage, reconstruction speed, image quality parameters, helium levels, temperature, humidity, and system error code information, acquisition parameter settings, system maintenance information	HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R.) Part 164, Standards for Privacy of Individually Identifiable Health Information Privacy Act of 1974, 5 U.S.C. § 552a, as amended, System of Record Notice, Patient Medical Record- VA 24VA10A7; Routine Use #29 VA Claims Confidentiality Statute, 38 U.S.C § 5701	Site to Site VPN Tunnel	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	owned by Philips Healthcare.	i.e. scan time, kV, mA, X-ray tube heat. Patient images are also transmitted for image artifact troubleshooting, which may include patient demographic data or Personal Identification Information (PII). Philips Healthcare will scrub data for any PII before assessments and before the data goes into the log files. The files are then purged. Data Flow Description: IPsec site-to-site VPN tunnel to			

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
		establish a secure connection for services provided by RSN to remotely diagnose, repair, monitor and update various VA networked medical devices and clinical information systems.			
ScriptPro LLC & ScriptPro USA	The purpose of this agreement section is to establish a management agreement between VA and ScriptPro regarding the development, management, operation and security of a connection between scriptpro SPCentral System, Owned by the	Prescription Data that may include Personally Identifiable Information (PII) or (PHI), Non-Identifiable Information, VA Facility Code, receiving facility address, Assigning Facility ID, ordering facility	HIPPA Privacy Rule 45, Code of federal Regulations (CFR) part 164, Standard for Privacy of Individually Identifiable Health Information, Privacy Act of 1974, 5 USC 552a as amended, 24VA10P2, Medical Records-VA Routine Use #29	Site to Site	Area Spokane-Walla Walla

List External Program Office or IT System information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT System	List the specific data element types such as PII/PHI that are shared/received with the Program or IT System	List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data	Applicable Sites within Area (VBA, VHA, NCA, Program Office)
	VA, and Script Pro's Technical Support Services Owned by ScriptPro.	address, De-identified information, Patient Identifiers (SSN, DOB) Unique Identifier (Facility Address, assigning facility, ordering provider address, Data logs (in text format)			
Siemens Healthcare Diagnostics Inc / Siemens Medical Solutions Inc	The purpose of this document is to establish a management agreement between Department of Veterans Affairs and Siemens Healthcare Diagnostics Inc / Siemens Medical Solutions Inc (Siemens Medical Solutions Inc). regarding the development,	Information Type Transmitted: Central Laboratory Diagnostics transmits laboratory instrument parameters, such as Central Processing Unit (CPU) resource utilization, water tank level, and probe counts. On rare	HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R.) Part 164, Standards for Privacy of Individually Identifiable Health Information Privacy Act of 1974, 5 U.S.C. § 552a, as amended; Patient Medical Record- VA 24VA10A7 Routine Use #29. VA Claims Confidentiality Statute, 38 U.S.C § 5701 (e)	Site to Site VPN Tunnel	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	<p>management, operation, and security of a system interconnection between Siemens Central Laboratory Diagnostics, RAPIDComm, AUWi-WAM, Siemens Imaging, owned or leased by Department of Veterans Affairs, and Medicalis Workflow Orchestrator systems and Smart Remote Services, owned or leased by Siemens Medical Solutions Inc. This agreement will govern the relationship between Department of Veterans Affairs and</p>	<p>occasions, where initiated by a VA employee for troubleshooting purposes, the data may include limited Protected Health Information (PHI) datasets (e.g. patient name, test results, medical record number, patient identifier, and accession number). Data Flow Description: From the VA systems to Siemens, over the peer to peer IPsec VPN, the transmission of this data primarily comes from the system</p>			

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	Siemens Medical Solutions Inc., including designated managerial and technical staff, in the absence of a common management authority.	residing at the VA. On occasion data in the form of updates will come from Siemens to the VA. This data flow includes system properties (software versions, system uptime, CPU/memory utilization, etc.) are transferred from Central Laboratory Diagnostics to Siemens via the interconnection on a predefined schedule. Files (communication logs, software update packages, etc.,) are transferred			

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
		from Siemens to the VA systems, over the peer to peer IPsec VPN, on an as-needed basis for troubleshooting or support purposes.			
Social Security Administration	The purpose of this agreement section is to establish a management agreement between VAIC and SSA regarding the development, management, operation, and security of a connection between the VAIC owned IPS and the SSA owned Enterprise Area-Wide Network (EWANS).	Information Type Transmitted: The data exchange contains PII information which include the following fields: SSNs, Last Name, Middle Initial, First Name, Date of Birth, Access Code, and VA record code and file number. Data Flow Description: The data flow bidirectional over a VPN	HIPAA Privacy Rule, 45 C.F.R. Part 164, Standards for Privacy of Individually Identifiable Health Information Privacy Act of 1974, 5 U.S.C. § 552a, as amended VA Claims Confidentiality Statute, 38 U.S.C § 5701 Confidentiality of Certain Medical Records, 38 U.S.C. § 7332 Freedom of Information Act, 5 U.S.C. § 552 U.S. Statute 38 U.S.C § 5106	Site to Site Bi-Directional VPN Tunnel	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
		tunnel via port 1364.			
Somnoware Healthcare Systems, Inc.	The purpose of this document is to establish a management agreement between Veterans Health Administration (VHA) and Somnoware Healthcare Systems, Inc. regarding the development, management, operation, and security of a system interconnection between Veterans Health Information System Technology Architecture (Vista), owned or leased by Veterans Health Administration, and Somnoware Software as a	Information Type Transmitted: Protected Health Information (PHI) Demographics of patients referred for respiratory and sleep disorder consultation and testing, International Code of Diseases (ICD10) diagnosis codes, Last four (4) digits of Social Security number (SSN), Continues Positive Airway Pressure (CPAP) device prescriptions Data Flow Description:	HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R.) Part 164, Standards for Privacy of Individually Identifiable Health Information Privacy Act of 1974, 5 U.S.C. § 552a, as amended; Patient Medical Record-VA; 24VA10A7; Routine Use #29. VA Claims Confidentiality Statute, 38 U.S.C § 5701	SAAS cloud via VPN	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	Service (SaaS), owned or leased by Somnoware Healthcare Systems, Inc.	Data is transmitted via HTTPS API calls over a Server-to-Server secure VPN connection. FIPS 140-2 compliant connection certificate number FIPS 3479.			
Sorna Corporation (Sorna)	The purpose of this agreement section is to establish a management agreement between the VA and Sorna Corporation regarding the development, management, operation, and security of a connection between Sorna CD/DVD Production System, owned by the VA, and Sorna Technical Services	Data to be transferred from the VA sites to Sorna would include software code trace files, machine language trace files, network packet captures, and DICOM protocol language to assist in the analysis of system troubleshooting issues. Patient information may be	HIPAA Privacy Rule, 45 C.F.R. Part 164, Standards for Privacy of Individually Identifiable Health Information Privacy Act of 1974, 5 U.S.C. § 552a, System of Records Notice 24VA10P2 Patient Medical Record – VA Routine Use #29. VA Claims Confidentiality Statute, 38 U.S.C § 5701	Site to Site	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	Department, owned by Sorna Corporation.	included in the DICOM communication, on purpose, if said data is included in the DICOM Header and if Sorna requires the DICOM Dataset to troubleshoot any issue the VA is encountering with the dataset.			
Cerner Corporation	The purpose of this MOU/ISA is to establish a configuration management agreement between VA and Cerner Corporation.	Information Type Transmitted: No Personally Identifiable Information (PII), Protected Health Information (PHI), or VA Sensitive Information is transmitted as part of this agreement. Upon CCE TS startup the CCE Terminal	There is no PHI transmitted therefore there are no privacy requirements	(Med-COI) Internet Protocol Security (IPsec) Tunnel	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
		<p>Server will receive image updates if needed.</p> <p>Data Flow Description: The CCE Terminal Server on each reboot sends a request via the CareAware application through the Joint Security Architecture (JSA) through the Med-COI IP Security (IPsec) tunnel to the Cerner iBus to see if there are any configuration changes since it's last reboot. If iBus identifies a requirement to update the configuration baseline, then iBus sends a response back to the CCE TS to initiate</p>			

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
		<p>a configuration update. The CCE TS upon notification from iBus that a configuration update is required will initiate a 443 GET from the AWS ECR/S3 which is a configuration repository that is hosted in the Cerner provided commercial AWS instance.</p>			
<p>Defense Health Agency (DHA)</p>	<p>The Parties require connectivity of authorized VA Sites and Med-COI deployed forward-deployed shared system components related to the Med-COI network for mission-critical enterprise</p>	<p>HL7, ICD-10, PHI, PII, and CUI with High Sensitivity</p>	<p>The Veterans Health Administration (VHA) is the only VA covered entity under 45 CFR 160.103 and VHA Directive 1605, VHA Privacy Program April 11,2012. VA as a business associate under the HIPPA regulations provides</p>	<p>TIC Gateways Secure Tunnel / Direct Tunnel PaloAlto Firewalls</p>	<p>Area Spokane-Walla Walla</p>

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	<p>healthcare delivery and business operations for the national deployment and implementation of DoD/VA joint capabilities (such as EHR, logistics, etc.) through authorized interagency transport mechanisms. This ISA does not document individual system-to-system interconnections. Such connections shall be documented in accordance with the use cases in Section 5.1.1 of the Med-COI MOA (i.e., connections involving a</p>		<p>information technology systems and support to VHA subject to the requirement of VA Directive 6066, PHI and Business Associate Agreements Management September 2, 2014. VA's System contain VHA PII Subject to the requirements of the Privacy Act and VHA Directive 1605.01. DHAs systems contain PII subject to the requirements of the Privacy Act of 1974, 5 US Code 552a, DOD 5400.11-R, DOD Privacy Program, and DOD Directive 5400.11</p>		

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	Major Program or System such as the EHR shall be documented in the DHA-VA EHR ISA).				
Internal Revenue Service	The purpose of this agreement section is to establish a management agreement between VHA and IRS regarding the development, management, operation, and security of a connection between the VHA's Connect Direct-IBM Mainframe, owned by VHA, and the IRS's Masterfile IBM Mainframe, owned by IRS.	A data file is compiled with names and social security numbers of veterans and spouses for the individuals on which the VA is requesting data. VHA then sends the data file to IRS and requests income information for each record/person for a particular tax year. The tax year is entered via parameter. When IRS receives the data file from VHA, it runs a match	Computer Matching Agreement (CMA) for the Disclosure of Information to Federal, State and Local Agencies (DIFSLA) regarding Tax Years 2009-2010 entered into by the Parties in 2011, The exchange of data per this Agreement is contingent upon the CMA taking effect. Section 6103(l)(7) of the Internal Revenue Code (I.R.C. 6103(l)(7)). I.R.C. Section 6103(l)(7)(D)(viii)(I) any needs-based pension provided under Chapter 15 of Title 38, U.S.C., or under any other law administered by the Secretary of Veterans Affairs;	Direct Secure Plus File Transfer software through a VA Transport Layer Protocol site-to-site VPN tunnel	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
		<p>against the information in its Masterfile system and generates a return file for VHA. Upon receipt of the return file from IRS that supplies tax return information for identified individuals from VHA's data file, VHA runs a match.</p>	<p>and 6103(l)(7)(D)(viii)(II) parents' dependency and indemnity compensation provided under 38 U.S.C. § 1315. 89VA10NB "Income Verification Records-VA" is the new SORN number and was effective as of January 21, 2014, document citation 78 FR 76897.VHA Veteran Eligibility for Medical Benefits "Income Verification Records-VA" (89VA16), first published 59 FR 8677 (Feb. 23, 1994), and last amended by 73 FR 31918 (June 4, 2008). IRS Unearned Income Return Information: Information Return Master File (IRMF)/IRS 22.061, as</p>		

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
			published at 73 FR 13302 (March 12, 2008), through the Disclosure of Information to Federal, State and Local Agencies (DIFSLA) program.		
Topcon Medical Systems	The purpose of this agreement section is to establish a management agreement between VA and Topcon Medical Systems regarding the development, management, operation, and security of a connection between VA's TRC-NW8 ImageNet Lite Imaging System, owned by VA, and Topcon network owned by Topcon Medical Systems.	Information Type Transmitted: No sensitive data is transmitted; the connection will be used to transfer and support of proprietary application software. Data Flow Description: Remote support only if necessary is via VPN from Topcon to VA. No data is collected, transmitted and/or stored.	<ul style="list-style-type: none"> • HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R.) Part 164, Standards for Privacy of Individually Identifiable Health Information [Add specific HIPAA provisions where applicable] • Privacy Act of 1974, 5 U.S.C. § 552a, as amended • VA Claims Confidentiality Statute, 38 U.S.C § 5701 • Confidentiality of Certain Medical Records, 38 U.S.C. § 7332 • Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. § 5705 • Freedom of 	Site to Site	Spokane Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
			Information Act (FOIA), 5 U.S.C. § 552		
IZ Gateway - CDC	The Cerner Electronic Health Record (EHR) has built-in functionality to query and report immunization data with a state/territorial IIS (signed agreement and Veteran authorization still required).	Name, Date of Birth, Immunization Records.	Covered under the data sharing agreement with Cerner EHRM / MEDMOD / CDC	Site to Site / DHA / Cerner Enclave routing	Area Spokane-Walla Walla
Centers for Disease Control and Prevention	The purpose of this agreement section is to establish a management agreement between VA OIT and CDC regarding the development, management, operation, and security of a connection between VDIFEP, owned by VA	Information Type Transmitted: VA OIT (VDIF-EP) data to CDC for testing and ultimately Production, contains Personal Information Identification (PII), Protected Health Information	HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R.) Part 164, Standards for Privacy of Individually Identifiable Health Information • Privacy Act of 1974, 5 U.S.C. § 552a, as amended • Virtual Lifetime Electronic Record (VLER) – VA 168VA10P2; Routine Use #11	Firewall Waiver, SFTP port 22	Area Spokane-Walla Walla

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
	OIT, which is located in the VA Enterprise Cloud (VAEC) and is hosted by Amazon Web Services (AWS), and the CDC BioSense Secure File Transfer Protocol (SFTP) server, owned by CDC, which is located in the AWS GovCloud environment.	(PHI), or VA sensitive information. VDIF-EP transfers patient encounter containing syndromic data in an encrypted file to CDC BioSense SFTP server (Document detailing the syndromic data elements is available upon request), for the purpose of establishing an integrated national public health surveillance system for early detection and rapid assessment of potential bioterrorism related illness. FOR OFFICIAL	FOR OFFICIAL USE ONLY 3 OFFICE OF INFORMATION SECURITY • Patient Medical Record- VA 24VA10P2 Routine Use 29 • VA Claims Confidentiality Statute, 38 USC 5701 (e)		

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT System</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT System</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
		USE ONLY 4 OFFICE OF INFORMATION SECURITY • Data Flow Description: The data is transmitted by the VA OIT developed data file via a Secure File Transfer Protocol (SFTP) connection to CDC BioSense SFTP server using public-key cryptography.			
EDRS	Pending MOU / ISA	Pending MOU / ISA	Pending MOU / ISA	Pending MOU / ISA	Area Spokane-Walla Walla

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

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

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

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

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

Follow the format below:

Privacy Risk: The sharing of data is necessary for individuals to receive benefits at the Area Spokane-Walla Walla. 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 and memorandums of understanding 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 screening or 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, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice in [Appendix A](#). (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the facilities within the Area 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 of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

The Area Spokane-Walla Walla 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 [VA System of Record Notices](#) (VA SORN) in the Federal Register and online.

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	Applicable SORs
VHA	<ul style="list-style-type: none"> • Non-VA Fee Basis Records-VA, SOR 23VA10NB3 • Patient Medical Records-VA, SOR 24VA10A7 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA10 • 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 79VA10 • Income Verification Records-VA, SOR 89VA10NB • Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA131 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10 • National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147-VA10NF1VHA Corporate Data Warehouse- VA 172VA10A&

<i>Site Type: VBA/VHA/NCA or Program Office</i>	<i>Applicable SORs</i>
	<ul style="list-style-type: none"> • Health Information Exchange - VA 168VA005
Special Purpose Systems	<ul style="list-style-type: none"> • Applicants for Employment Under Title 38 – VA SOR 02VA135 • Employee Medical File System Records – VA SOR 08VA05 • Patient Advocate Tracking System Replacement (PATs-R) – VA SOR 100VA10H • Police and Security Records – VA SOR 103VA07B • Compliance Records, Response, and Resolution of Reports of Persons Allegedly Involved in Compliance Violations – VA SOR 106VA17 • Enrollment and Eligibility Records – VA SOR 147VA10 • Customer Relationship Management System (CRMS) – VA SOR 155VA10NB • VHA Corporate Data Warehouse – VA SOR 172VA10 • Non-VA Care (Fee) Records – VA SOR 23VA10NB3 • Patient Medical Records – VA SOR 24VA10A7 • Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA SOR 54VA10NB3 • Community Placement Program – VA SOR 65VA122 • Health Care Provider Credentialing and Privileging Records – VA SOR 77VA10A4 • Veterans Health Information Systems and Technology Architecture (VistA) Records – VA SOR 79VA10 • Automated Safety Incident Surveillance and Tracking System – VA SOR 99VA13 • HealthShare Referral Manager (HSRM) – VA SOR 180VA10D • Community Care (CC) Provider Profile Management System (PPMS) – VA SOR 186VA10D • Veteran, Patient, Employee, and Volunteer Research and Development Project Records – VA SOR 34VA10 • National Patient Databases – VA SOR 121VA10A7

This Privacy Impact Assessment (PIA) also serves as notice of the Area Spokane-Walla Walla 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.

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 Spokane-Walla Walla 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 Spokane-Walla Walla.

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	<p>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.</p> <p>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.</p> <p>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.</p>

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

An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SOR. If an individual does not know the "office concerned," the request may be addressed to the 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 <https://www.va.gov/find-forms/about-form-10-5345a/>.

Additionally, veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the my [HealthVet program](#), VA’s online personal health record. More information about my HealthVet is available at <https://www.myhealth.va.gov/index.html>.

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.

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

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

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

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

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

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

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information.

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

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

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

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

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

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA).

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

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

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

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

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

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

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

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

Follow the format below:

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

Mitigation: Area Spokane-Walla Walla 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 there is a major change. The NOPP discusses the process for requesting an amendment to one's records.

The Area Spokane-Walla Walla Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information. The Veterans' Health Administration (VHA) established MyHealthVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

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

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

Identify users from other agencies who may have access to the Area and under what roles these individuals have access to the Area. 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. 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 Design and Development.

Individuals receive access to the Area Spokane-Walla Walla 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 Spokane-Walla Walla 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 (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 Spokane-Walla Walla 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 Spokane-Walla Walla 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 Officer (ISSO), local Area Manager, System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

Human Resources notifies Services, IT, TMS Coordinator, and ISSO of new hires and their start date(s) through e-mail notification of New Employee Orientation (NEO). New hires' computing equipment and network account creation is initiated via Human Resources or the Service through the Service Now (SNOW) – User Provisioning portal, managed by the Enterprise Service Desk (ESD). The SNOW ticket generates notification to the Area Manager or designee for equipment provisioning, which is then approved, modified, or disapproved as appropriate. ESD creates the network account (Active Directory, "AD"), SIP account, and Exchange server account. Local OIT staff modifies the AD account as appropriate once created. The Service that receives new hire request notifications, submits via YourIT ticket, any Cerner User Role for the assigned position, as well as access to any shared folder requirements, and access to applications not included in VA's imaging process that the new hire will require. Documentation is filed in an employee folder and is also maintained electronically by 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.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the Area 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 after completing the VA Privacy and Information Security Awareness training and 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 reviewed by 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 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 information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy. Contractors with VA Area Spokane-Walla Walla access must have an approved computer access request on file. The area manager, or designee, in conjunction with the 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 program or Area?

VA offers privacy and security training. Each program or Area may offer training specific to the program or Area 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 Spokane-Walla Walla personnel, volunteers, and contractors are required to complete initial and annual Privacy and Security Awareness and Rule Behavior (RoB) training, during New Employee Orientation (NEO) or via TMS. In addition, all employees who interact with patient sensitive medical information must complete the Privacy and HIPAA focused mandated privacy training. Finally, all new employees receive face-to-face training by the Area Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officers also perform subject specific trainings on an as needed basis.

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

VA 10176: Privacy and Information Security Awareness and Rules of Behavior

VA 10203: Privacy and HIPPA Training

VA 3812493: Annual Government Ethics.

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

8.4a If Yes, provide:

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

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

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

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 Design and Development
AR-8	Accounting of Disclosures
DI	Data Quality and Integrity
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	Data Minimization and Retention
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	Individual Participation and Redress
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	Security
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	Transparency
TR-1	Privacy Notice
TR-2	Area 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 Officers

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

Privacy Officer, Nicholas Quinn

Privacy Officer, Harvey H. Howell

Information System Security Officer, Douglas K. Bell

Information System Security Officer, Joseph Hoffman

Area Manager, Scott Brown

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

<i>Site Type: VBA/VHA/NCA or Program Office</i>	<i>Applicable NOPPs</i>
VHA	<u>Notice of Privacy Practices</u> <u>VHA Privacy and Release of Information:</u>

APPENDIX B – PII Mapped to Components

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

PII Mapping of Components (Servers/Database)

<i>Components of the Area collecting/storing PII (Each row refers to a grouping of databases associated with a single server)</i>	<i>Does this component collect PII? (Yes/No)</i>	<i>Does this component store PII? (Yes/No)</i>	<i>Does this component share, receive, and/or transmit PII? (Yes/No)</i>	<i>Type of PII (SSN, DOB, etc.)</i>	<i>Reason for Collection/ Storage of PII</i>	<i>Safeguards</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
Server 1: OITSPOSQLO16 <ul style="list-style-type: none"> • Censis_Beta_V2_Global • censis_graphics • Censis_HL1319 • Censis_SG1319 • CensisBufferAgent • DLM • EncoreDB • EncoreWarehouse • FaxQueue2k • hibernate • jackrabbit • mipacs_db • mipacsTEST_db • NOAHDatabaseCore • QCDAO • qp_agent • qp_app 	Yes	Yes	Yes	PII / PHI / FIN / EDIPI, Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s) Fax Number, E-mail Address, Financial Account Information, Current	To provide and manage benefits for the veteran	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	Spokane VAMC (VHA)

<i>Components of the Area collecting/storing PII (Each row refers to a grouping of databases associated with a single server)</i>	<i>Does this component collect PII? (Yes/No)</i>	<i>Does this component store PII? (Yes/No)</i>	<i>Does this component share, receive, and/or transmit PII? (Yes/No)</i>	<i>Type of PII (SSN, DOB, etc.)</i>	<i>Reason for Collection/ Storage of PII</i>	<i>Safeguards</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
<ul style="list-style-type: none"> • qp_auditing • qp_calendar • qp_central • quartz • SilhouetteCentral • SilhouetteCentralTest • SPO_BioPoint_PI6 • statdb • WorkflowLog2k • DLM • FaxQueue2k • WorkflowLog2k 				Medications, Previous Medical Records, Race/Ethnicity/Gender, Electronic Protected Health Information			
<p>Server 2: OITSP0SQL019</p> <ul style="list-style-type: none"> • BHL_SPO_Prod • BHL_SPO_Test • CentrakWPS • Compass • EMR • NARS • SFFX • SmithsSolisE • SPOMedManager 	Yes	Yes	Yes	PII / PHI / FIN / EDIPI, Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s) Fax Number, E-mail	To provide and manage benefits for the veteran	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	Spokane VAMC (VHA)

Components of the Area 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	Applicable Sites within Area (VBA, VHA, NCA, Program Office)
				Address, Financial Account Information, Current Medications, Previous Medical Records, Race/Ethnicity/Gender, Electronic Protected Health Information			
<p>Server 3: OITWWWSQL016</p> <ul style="list-style-type: none"> • DLM • FaxQueue2k • NOAHDatabaseCore • SilhouetteCentral 	Yes	Yes	Yes	PII / PHI / FIN / EDIPI, Name, Social Security Number, Date of Birth, Mailing Address, Zip	To provide and manage benefits for the veteran	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with	Walla Walla VAMC (VHA)

Components of the Area 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	Applicable Sites within Area (VBA, VHA, NCA, Program Office)
<ul style="list-style-type: none"> • SilhouetteCentralTest • WorkflowLog2k • zzHL7 • zzNew • zzOld • zzPat • DLM • FaxQueue2k • WorkflowLog2k 				Code, Phone Number(s) Fax Number, E-mail Address, Financial Account Information, Current Medications, Previous Medical Records, Race/Ethnicity/Gender, Electronic Protected Health Information		restricted access controls	
<p>Server 4: OITWWWSQL019</p> <ul style="list-style-type: none"> • BHL_WWW_Prod • BHL_WWW_Test • Censis_Beta_V2_Global • censis_graphics 	Yes	Yes	Yes	PII / PHI / FIN / EDIPI, Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone	To provide and manage benefits for the veteran	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	Walla Walla VAMC (VHA)

Components of the Area 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	Applicable Sites within Area (VBA, VHA, NCA, Program Office)
<ul style="list-style-type: none"> • Censis_HL2024 • Censis_SG2024 • CensisBufferAgent • CompassWWW • EMR • SFFX 				Number(s) Fax Number, E-mail Address, Financial Account Information, Current Medications, Previous Medical Records, Race/Ethnicit y/Gender, Electronic Protected Health Information			
<p>Server 5: WWW-LT29183 \UPSW2019SERVER</p> <ul style="list-style-type: none"> • Upslpmdb • UPSNrfRVLDB • UPSNrfUserDB • upswsdb • upswsdb_ActivityLog • upswsdb_reconciler 	Yes	Yes	Yes	Name, Fax Number, E- mail Address, Financial Account Information, Merchandise Description	To provide and manage benefits for the veteran	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	Walla Walla VAMC (VHA)

Components of the Area 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	Applicable Sites within Area (VBA, VHA, NCA, Program Office)
upswsdb_report							
Server 6: WWW-LT29376 \UPSW2019SERVER <ul style="list-style-type: none"> • Upslpmdb • UPSNrfRVLDB • UPSNrfUserDB • upswsdb • upswsdb_ActivityLog • upswsdb_reconciler upswsdb_report 	Yes	Yes	Yes	Name, Fax Number, E-mail Address, Financial Account Information, Merchandise Description	To provide and manage benefits for the veteran	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	Walla Walla VAMC (VHA)
Server 7: WWW-LT30528 \UPSW2019SERVER <ul style="list-style-type: none"> • Upslpmdb • UPSNrfRVLDB • UPSNrfUserDB • upswsdb • upswsdb_ActivityLog • upswsdb_reconciler upswsdb_report 	Yes	Yes	Yes	Name, Fax Number, E-mail Address, Financial Account Information, Merchandise Description	To provide and manage benefits for the veteran	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	Walla Walla VAMC (VHA)
Server 8: WWW-WS29534 \UPSW2019SERVER <ul style="list-style-type: none"> • Upslpmdb 	Yes	Yes	Yes	Name, Fax Number, E-mail Address, Financial	To provide and manage benefits for the veteran	Advanced Encryption Standard (AES) 256, Server is	Advanced Encryption Standard (AES) 256,

<i>Components of the Area collecting/storing PII (Each row refers to a grouping of databases associated with a single server)</i>	<i>Does this component collect PII? (Yes/No)</i>	<i>Does this component store PII? (Yes/No)</i>	<i>Does this component share, receive, and/or transmit PII? (Yes/No)</i>	<i>Type of PII (SSN, DOB, etc.)</i>	<i>Reason for Collection/ Storage of PII</i>	<i>Safeguards</i>	<i>Applicable Sites within Area (VBA, VHA, NCA, Program Office)</i>
<ul style="list-style-type: none"> • UPSNrfRVLDB • UPSNrfUserDB • upswsdb • upswsdb_ActivityLog • upswsdb_reconciler • upswsdb_report 				Account Information, Merchandise Description		stored in a secured environment and managed with restricted access controls	Server is stored in a secured environment and managed with restricted access controls

APPENDIX C – List of Special Purpose Systems

Name of Special Purpose Systems
Area Spokane-Walla Walla SPS