Date PIA submitted for review:

07/27/2022

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

Area Wichita

District Midwest

Facilities Supported by the Area

Facilities Supported by the Area:
1. Robert J Dole VAMC
2. Wichita VA Regional Center Office
3. Vet Center
4. Community Based Outpatient (Hays KS, Dodge City KS, Salina KS, Parsons KS)

---

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

Area Boundary Contacts:

Area Privacy Officer

Name	Phone Number	Email Address	Location
Designated Area PO (The PO located in the same VAMC as the Area Manager): Keith Hall	316-688-6892	Keith.hall@va.gov	Area Wichita
Andrew Freeman	316-688-6887	Andrew.freeman5@va.gov	Area Wichita

Area Information System Security Officer

Name	Phone Number	Email Address	Location
Designated Area ISSO: (The ISSO located in the same VAMC as the Area Manager): Rolando Trevino	316-368-5585	Rolando.trevino@va.gov	Area Wichita
David Shaw	316-688-6749	David.shaw4@va.gov	Area Wichita

Area Manager

Name	Phone Number	Email Address	Location
Jason Parker	316-469-0900	Jason.Parker@va.gov	Area Wichita

Abstract

Area Wichita is an Information Area Boundary that consists of Robert J Dole Medical Center, Wichita Regional Office and the community-based outpatient clinics in Salina, KS; Hays, KS; Hutchison, KS; Parsons, KS; Dodge City, KS as well as the Vet Center in Wichita KS. The Area Boundary environment consists of components such as workstations, laptops, portable computing devices, terminals, servers, printers, and IT enabled networked medical devices that are owned, managed, and maintained by the facilities. The Area provides operational connectivity services necessary to enable users' access to information technology resources throughout the enterprise including those within the facility, between facilities, resources hosted at data centers, and connectivity to other systems. Network connectivity rules are enforced by VA approved baselines for router and switch configurations. The Area Boundary system environment also includes as applicable, subsystem storage utilities such as tape drives, optical drives, disk drives, network area storage (NAS), storage access networks (SAN), archival appliances, special purpose systems, and tier 2 storage solutions. The Area Boundary encompasses the management, operational, and technical security controls associated with IT hardware, consisting of servers, routers, switches, hubs, gateways, peripheral devices, desktop/laptops, and OS software. The Area Boundary employs a myriad of routers and switches that connect to the VA network.

Overview

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

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

[Please pay attention to the bulleted questions above and make sure each question is addressed in the Overview response.]

Area Wichita directly supports the Veterans Health Administration mission of providing care to our nation's Veterans and eligible beneficiaries as well as the Veterans Benefits mission of providing benefits and services to eligible Veterans, their families, and beneficiaries.

The Area Wichita consists of computing resources/server platforms associated with the clinical and administrative operations necessary to support the Robert J. Dole VA Medical Center and the community-based outpatient clinics in Salina, KS.; Hays, KS.; Hutchison, KS.; Parsons, KS.; Dodge City, KS.; Vet Centers in Wichita, KS.; and the Wichita VA Regional Office (RO) in Wichita, KS. VA staff issued VA Personal Identity Verification (PIV) credentials working at these sites have access to these IT computing resources, e.g., all IT hardware including servers, printers, scanners and all other peripheral devices, desktop computer systems, mobile computing devices, medical devices and all operating systems software currently installed thereon. The Area Wichita is continuously used during normal business and non-business hours, supporting many processes. Area Wichita serves as the default repository for incidental data used and processed by various VBA Major Applications maintained at the Enterprise level. This data is used in granting compensation, pension, education and vocational rehabilitation, and employment to Veterans. Information stored also includes data used for various administrative functions. The system provided RO employees local access to file and print sharing services. It also provided client access to various applications, including email. The confidentiality, integrity, and availability of the Area Wichita system is critical, i.e., ensuring that data is only received by the persons and applications that it is intended for, that data is not subject to unauthorized or accidental alterations, and that the resources are available when needed.

VHA, and VBA Facilities located within the Area Wichita IT Boundary all access VA Enterprise IT systems respectively, hosted and maintained outside of this boundary. These are VISTA, VBMS, MEM, etc. operating systems software currently installed thereon. The Area Wichita is continuously used during normal business and non-business hours, supporting many processes. The confidentiality, integrity, and availability of the Area Providence system is critical, i.e., ensuring that data is only received by the persons and applications that it is intended for, that data is not subject to unauthorized or accidental alterations, and that the resources are available when needed Applications and devices within the Area Wichita.
Only PII/PHI collected and used by the facilities within the Area will be referenced in this document since the Area IT boundary does not maintain, disseminate or store information accessed by each facility. PII/PHI. All repositories used by the facilities are at the enterprise level with the exception of medical devices.
Area Wichita is sharing information externally with Social Security Administration, Internal Revenue Service, and other systems as listed in table 5.1.

The legal authorities to operate as outlined in Section 1.6 include Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Privacy Act of 1974, and Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b)
Completion of this Privacy Impact Assessment will not result in any business or technology changes.
The Area is using the VA Enterprise Cloud (VAEC) which is at the enterprise level and is outside of the Area boundary. Further information can be found in the VAEC PIA.
The facilities within the Area IT Boundary collect, use, and/or disseminate PII/PHI that is maintained and stored within enterprise systems such as VistA, VBMS, BOSS/AMASS, etc. There are individual PIAs located here (https://www.oprm.va.gov/privacy/pia.aspx) 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 applicable SORs for Wichita Area include:

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

Section 1. Characterization of the Information

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name
☒ Personal Mailing Address

☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone

Number, etc. of a different individual)
☒ Financial Account Information
☒ Health Insurance Beneficiary Numbers Account numbers

☒ Certificate/License numbers
☒ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Current Medications
☒ Previous Medical Records
☒ Race/Ethnicity

☐ Tax Identification Number
☐ Medical Record Number
☒ Next of Kin

☒ Guardian Information
☒ Electronic Protected Health Information (ePHI)
☒ Military History/Service Connection
☒ Service-connected Disabilities
☒ Employment Information
☒ Veteran Dependent Information
☒ Disclosure Requestor Information

☒ Death Certification Information
☒ Criminal Background
☒ Education Information
☒ Gender
☐ Tumor PHI Statistics
☒ Other Unique Identifying Information (list below)

PII Mapping of Components

Area Wichita consists of 102 key components (servers/databases) that house data. Upon review of the key components only 12 (servers/database) contains PII. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected within Area Wichita and the reasons for the collection of the PII are in the **Mapping of Components Table in Appendix B of this PIA.**

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

The information that resides within the facilities in the Area Boundary is collected, maintained, and/or disseminated comes from a variety of sources. The largest amount of data comes directly from individuals - including veterans and their dependents, volunteers and other members of the public, clinical trainees, and VA employees and contractors. For example: items such as names, social security numbers, dates of birth are collected from the individual on healthcare enrollment forms (VA Form 10-10EZ), or other paperwork the individual prepares. An application for employment contains the same, or similar, information about employees.

Depending on the type of information, it may also come from 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.

Additional sources include:

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

1.3 How is the information collected?

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.
VBA	There are many VA forms used by Veterans to apply for and/or make adjustments to pending benefits. All VBA benefit forms are located at http://www.va.gov/vaforms/. The URL of the associated privacy statement is: http://www.va.gov/privacy/. VBA forms can be downloaded from this site, filled in and printed to be delivered in paper form. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury. The VBA toll free number for veterans is 1-800-827-1000. Clients are referred to and transferred to the Regional Office of Jurisdiction, where they can provide a service representative with required information. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury. VBA employees may also contact a Veteran directly to obtain clarifying information for a claim for benefits.

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 Wichita using several methods such as electronic transmission, verbally, email, fax, or can be created by the individual in form of a letter. 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. The information is collected from the individual, other legal representative, VA Form DD 214, VA Form 10-10 (EZ, EC, HS CG), VA Form 0750, employee supervisors, providers, research activities, and contractors. Criminal record information and state drug prescription monitoring (MAPS) are accessed through the website using state portals. The website is used to connect to the HEC (Health Eligibility Center) and VBA databases for benefit and eligibility information. Information can be transmitted via encrypted email and facsimile (fax). Claims information is retrieved electronically. Various forms are used locally to collect information, which is transferred into CPRS (Computerized Patient Record System) and the form shredded. Various VA Forms are used, as follows: VA Form 10-2364 for Audiology Reports, SF 518 for Blood Transfusions, VA Forms 10-5345 & 10-5345a for Release of Information, VA Form 10-0539 Functional Categories, VA Form 10-2623 Proficiency Report, VA0233 Change of Address, VA0750 Performance Appraisal, VA127 Report of Survey, VA2235 List of Personally Owned Equip., VA2237 Request Turn-In & Receipt for Property or Services, ECF form, VA4659 Incentive Awards, VA 10-011R Fax Cover Sheet, VA4793 Visitor Registry, VA Form 2850, 10-2850a, 10-2850b, 10-2850c, OF 306, VA3963/3963a, SF144, CA-1, CA-2, NEPEC Form, local PIV Form, FMLA Paperwork, Uniform Officers Report..

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

The purposes of the information from Veterans and other members of the public collected, maintained, and processed by Area Wichita 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	• To determine eligibility for health care and continuity of care • Emergency contact information is cases of emergency situations such as medical emergencies • Provide medical care

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

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

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?

Legal Authority Table

Site Type: VBA/VHA/NCA or Program Office	Legal Authority
VHA	• 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.
VBA	• Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b)

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Privacy Risk:
VA Area Wichita 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 Wichita employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control, awareness and training, audit and accountability, certification, accreditation, and security assessments, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and system and information integrity. The area employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring

guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

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

Section 2. Uses of the Information

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

2.1 Describe how the information within the Area Boundary will be used in support of the program's business purpose.

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

- **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

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?

The VA Area Wichita uses statistics and analysis to create general reports that provide the VA a better understanding of patient care, benefits, 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

Letters to veterans concerning the progress of their claim are generated periodically, as well as rating decisions and requests for additional information to substantiate the claim. These letters are generated electronically and printed on paper and mailed to the veteran.

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

The controls in place to assure that the information is handled in accordance with the uses described above include mandatory online information security and Privacy and HIPAA training; face-to-face training for all incoming new employees conducted by the Information System Security Officer and Privacy Officer; regular audits of individuals accessing sensitive information; and formal administrative rounds during which personal examine all areas within the facility to ensure information is being appropriately used and controlled.

Section 3. Retention of Information

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

3.1 What information is retained by the facilities within the Area Boundary?

The Area Wichita Boundary 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

3.2 How long is information retained by the facilities?

Length of Retention Table

Site Type: VBA/VHA/NCA or Program Office	Length of Retention
VHA	- Financial Records: Different forms of financial records are retained 1-7 years based on specific retention schedules. Please refer to VA Record Control Schedule (RCS)10-1, Part Two, Chapter Four- Finance Management - Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)10-1, Part Three, Chapter Six- Healthcare Records, Item 6000.1a. and 6000.1d. - Official Human Resources Personnel File: Folder will be transferred to the National Personnel Records Center (NPRC) within 30 days from the date an employee leaves the VA. NPRC will destroy 65 years after separation from Federal service. (Department of Veterans Affairs Record Control Schedule (RCS)10-1, Part Two, Chapter Three- Civilian Personnel, Item No. 3000.1 - Office of Information & Technology (OI&T) Records: These records are created, maintained and disposed of in accordance with Department of Veterans Affairs, Office of Information & Technology RCS 005-1.
VBA	- Compensation, pension, and vocational rehabilitation claims folders are retained at the servicing regional office until they are inactive for three years, after which they are transferred to the Records Management Center (RMC) for the life of the Veteran. - Official legal documents (e.g., birth certificates, marriage licenses) are returned to the claimant after copies are made for the claimant's file. At the death of the Veteran, these records are sent to the Federal Records Center (FRC) and maintained by the National Archives and Records Administration (NARA) in accordance with NARA policy. - Once a file is electronically imaged and accepted by VBA, its paper contents (with the exception of documents that are the official property of the Department of Defense, and official

Site Type: VBA/VHA/NCA or Program Office	Length of Retention
	legal documents), are destroyed in accordance with Records Control Schedule VB–1 Part 1 Section XIII, as authorized by NARA.
	• Documents that are the property of the Department of Defense are either stored at the RMC or transferred to NARA and maintained in accordance with NARA policy.
	• Vocational Rehabilitation counseling records are maintained until the exhaustion of a Veteran's maximum entitlement or upon the exceeding of a Veteran's delimiting date of eligibility (generally, ten or twelve years from discharge or release from active duty), whichever occurs first, and then destroyed.
	• Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA.
	• Education electronic folders are retained at the servicing Regional Processing Office. Education folders may be destroyed in accordance with the times set forth in the Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA.
	• Employee productivity records are maintained for two years after which they are destroyed by shredding.

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

Retention Schedule Table

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

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

Information within the Area Wichita is destroyed by the disposition guidance of *[RCS 10-1, VB-1, etc.]*. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014)

Additionally, the Area Wichita follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014, for Media Sanitization Program, SOPs - FSS - All Documents **as well as** FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the **Department of Veterans' Affairs Directive 6500 VA Cybersecurity Program (January 23, 2019)**. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Directive 6500. Digital media is shredded or sent out for destruction per VA Directive 6500.

Paper records are shredded on-site by a shredding company, witnessed by the Records Management Officer, and are accompanied by a certificate of destruction. Non-paper records maintained on magnetic media are destroyed by erasing the magnetic media using an approved software to digitally overwrite the media. The media is then shredded on-site by the contracted shredding company, witnessed by the Records Management Officer per VBA Directive 6300.

3.5 Does the Area Boundary include any facility or program that, where feasible, uses techniques to minimize the risk to privacy by using PII for research, testing, or training?

Controls which are in place with regard to testing to minimize risk to privacy of using PII for testing include VA Technical Reference Model (TRM) Compliance Enforcement and Announcement of OIT Architecture and Engineering Review Board (AERB) VAIQ#7110943", dated July 1, 2011, compliance with the One-VA TRM is mandatory for any non-VA developed software which is deployed within VA's production network environment except for CIO exempted systems (i.e. medical devices), under VAIQ #7566605, Updated Security Requirements for Network Connected Medical Devices and Systems. This requirement is consistent with VA policy, including, but not limited to, VA Handbooks 6102 and 6500; VA Directives 6004, 6513, and 6517; and National Institute of Standards and Technology (NIST) standards, including Federal Information Processing Standards (FIPS). With regard to training all personnel on the facility staff or affiliated with the facility, who have access to PHI/PII are required to complete their privacy and information security training each year in an effort to minimize risk to privacy. For Research there are Data Use Agreements (DUA) in place with outside entities with whom the facility shares information with. In the research department of the facility there is a deliberate review process for all human related study projects which includes review of the research projects by the Privacy Officer and the Information Security Officer (ISO) using VA checklists to ensure the research projects are compliant with VA requirements with regard to PHI/PII.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Privacy Risk: There is a risk that the information maintained by Area Wichita 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 Wichita 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 Wichita 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 form 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 Boundary 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.

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

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT System*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
Veterans Benefits Administration (VBMS)	Filing benefit claims	Social Security Number, Benefits Information, Claims Decision, DD-214	Compensation and Pension Record Interchange (CAPRI) electronic software package	Wichita Regional Office; Robert J. Dole VA Medical Center
VistA	Electronic Health Record	Area Boundary Log files, sample clinical data that may contain Protected Health Information (PHI)	Electronically pulled from VistA thru Computerized Patient Record Area Boundary (CPRS)	Robert J. Dole VA Medical Center; CBOCs

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	Provide name of Applicable Area Sites
Veterans' Health Administration	VHA – Provide Care	System Log files, Name, Date of Birth, SSN, demographics, Protected Health Information (PHI), benefits/copay information, IP	Electronically pulled from VistA thru Computerized Patient Record System (CPRS)	Robert J. Dole VA Medical Center; CBOCs
Austin Automation Center (AAC)	Healthcare encounter information	Name, Date of Birth, Sex, SSN, demographics and health information	Information may be transmitted electronically. AAC employees can log into CPRS or VistA	Robert J. Dole VA Medical Center; CBOCs
Health Eligibility Center (HEC)	Healthcare encounter information	Name, Date of Birth, Sex, SSN, demographics and health information	Information may be transmitted upon request in an electronic, written or verbal format based on the individual request. Methods include electronically thru encrypted emails, mail of encrypted CDs, secure facsimile, via secure web portal, SharePoint, and direct electronic file sharing or hard copies via routine mail or courier	Robert J. Dole VA Medical Center; CBOCs
VA Veteran Centers	Continuity of care, eligibility, and enrollment		Electronically viewed through the Computerized	Robert J. Dole VA Medical Center; CBOCs

			Patient Record System (CPRS) or information may be transmitted upon request in an electronic, written or verbal format based on the individual request. Methods include electronically thru encrypted emails, mail of encrypted CDs, secure facsimile, via secure web portal, SharePoint, and direct electronic file sharing or hard copies via routine mail or courier	
Veteran's Service Organizations (VSO) – specific organization such as Veterans of Foreign War (VFW), etc.	The organization helps members apply for VA benefits	Pertinent PII, PHI, and III appropriate to the request	Information may be transmitted upon request in an electronic, written or verbal format based on the individual request. Methods include electronically thru encrypted emails, mail of encrypted CDs, secure facsimile, via secure web portal, SharePoint, and direct electronic file sharing or hard copies via routine mail or courier	Robert J. Dole VA Medical Center; CBOCs

	Information is shared requesting verification of death benefits	Pertinent PII, PHI, and III appropriate to the request	Information may be transmitted upon request in an electronic, written or verbal format based on the individual request. Methods include electronically thru encrypted emails, mail of encrypted CDs, secure facsimile, via secure web portal, SharePoint, and direct electronic file sharing or hard copies via routine mail or courier	Robert J. Dole VA Medical Center; CBOCs
Department of Veterans Affairs General Counsel Office	Assistance in investigation of patient or employee claims	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) appropriate to the request to include Name, SSN, DOB, financial information as it applies		
FOIAXpress	Documentation and tracking of Freedom of Information Act requests	Pertinent PII, PHI, and III appropriate to the request	Information is uploaded electronically to secure database website	Robert J. Dole VA Medical Center; CBOCs
Consolidated Patient Accounts Center (CPAC)	Coordinate third party billing and copayments	Pertinent PII, PHI, and III appropriate to the request	Information may be transmitted upon request	Robert J. Dole VA Medical Center; CBOCs

			in an electronic, written or verbal format based on the individual request	
VA Network Authorization Office Non-VA Care	VA Network Authorization Office Non-VA Care	Name, DOB, SSN, Demographics, supporting documentation and Medical Information	Sent via-Triwest secure electronic portal	Robert J. Dole VA Medical Center; CBOCs
VHA Support Services Center (VSSC)	Healthcare information, metrics and analysis	Name, Date of Birth, Sex, SSN, demographics and health information	Secure Electronic transmission (HTTPS)	Robert J. Dole VA Medical Center; CBOCs

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

<u>Privacy Risk:</u> The internal sharing of data is necessary individuals to receive benefits at the Area Wichita. 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.

<u>Mitigation:</u> 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.

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*	*List names of Applicable Area Sites*
Social Security Administration	Eligibility for Federal benefits	SSN, Name, Address	National ISA/ MOU	Site to Site (S2S), IPSEC Tunnel, Secure FTP	Robert J. Dole VA Medical Center; CBOCs; Wichita Regional Office
Internal Revenue Services	Income verification	Name, Financial Information	ISA/ MOU, Computer Matching Agreement	Secure Web-Portal, Secure Socket Layer	Robert J. Dole VA Medical Center; CBOCs; Wichita Regional Office
Department of Defense	Determine military service dates, eligibility	Name, Service Information, SSN	MOU	Bi-directional Health Information Exchange	Robert J. Dole VA Medical Center; CBOCs; Wichita Regional Office
American Veterans (AMVETS)	Veterans Benefits Claims Assistance	Name, DOB, SS#, address, dependents info, disabilities, medical information,	Veterans Benefits, Title 38, United States Code (U.S.C.),	Electronic transmission methods through Citrix Access Gateway	Wichita Regional Office

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	List names of Applicable Area Sites
		telephone number, benefits,	Chapter 5, § 501(b) SORN 58VA21/22/28	(CAG) if emote or controlled access to the local office GSS if physically co-located	
Kansas Commission on Veterans Affairs (KCVA)	Veterans Benefits Claims Assistance	Name, DOB, SSN, Address, Financial Information, Disability's	Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b) SORN 58VA21/22/28	Electronic transmission methods through Citrix Access Gateway (CAG) if emote or controlled access to the local office GSS if physically co-located	Robert J. Dole VA Medical Center; CBOCs;
Military Order of the Purple Heart (MOPH)	Veterans Benefits Claims Assistance	Name, DOB, SS#, address, dependents info, disabilities, medical information, telephone number, benefits, income, direct deposit info	Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b) SORN 58VA21/22/28 (February 14, 2019	Electronic transmission methods through Citrix Access Gateway (CAG) if emote or controlled access to the local office GSS if physically co-located	Wichita Regional Office

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	List names of Applicable Area Sites
American Legion (AL)		Name, DOB, SSN, Address, Financial Information, Disability's		Electronic transmission methods through Citrix Access Gateway (CAG) if emote or controlled access to the local office GSS if physically co-located	
Disabled American Veterans (DAV)	Veterans Benefits Claims Assistance	Name, DOB, SS#, address, dependents info, disabilities, medical information, telephone number, benefits, income, direct deposit info	Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b) SORN 58VA21/22/28 (February 14, 2019	Electronic transmission methods through Citrix Access Gateway (CAG) if emote or controlled access to the local office GSS if physically co-located	Wichita Regional Office
Veterans of Foreign Wars (VFW)	Veterans Benefits Claims Assistance	Name, DOB, SS#, address, dependents info, disabilities, medical information, telephone number, benefits, income, direct deposit info	Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b) SORN 58VA21/22/28	Electronic transmission methods through Citrix Access Gateway (CAG) if emote or controlled access to the local office	Wichita Regional Office

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*	*List names of Applicable Area Sites*
				GSS if physically co-located	

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

Follow the format below:
Privacy Risk: The sharing of data is necessary for individuals to receive benefits at the Area Wichita. 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 <u>Appendix A</u>. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	Applicable SORs
VHA	- Non-VA Fee Basis Records-VA, SOR 23VA10NB3 - Patient Medical Records-VA, SOR 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&

Site Type: VBA/VHA/NCA or Program Office	Applicable SORs
	• Health Information Exchange - VA 168VA005
VBA	• Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28

This Privacy Impact Assessment (PIA) also serves as notice of the Area Wichita. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

The VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans.

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

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

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

The Area Wichita 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 Wichita.

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

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

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

<u>Privacy Risk:</u> There is a risk that veterans and other members of the public will not know that the Area Wichita exists or that it collects, maintains, and/or disseminates PII, PHI or PII/PHI about them.

<u>Mitigation:</u> 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?

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 myHealth*e*Vet program, VA's online personal health record. More information about my Health*e*Vet is available at https://www.myhealth.va.gov/index.html.

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

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

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act 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?

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

Right to Request Amendment of Health Information.

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

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

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

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

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

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

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

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

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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 Wichita 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 Wichita Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.

The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

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

Individuals receive access to the Area Wichita 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 Wichita requires access to the GSS be requested using the local access request system. VA staff must request access for anyone requiring new or modified access to the GSS. Staff are not allowed to request additional or new access for themselves.

Access is requested utilizing Electronic Permission Access Area Boundary (ePAS). Users submit access requests based on need to know and job duties. Supervisor, ISSO and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need-to-know basis.

Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel. Access to computer rooms at VA Area Wichita 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 Wichita working and storage areas is restricted to VA employees who must complete both the HIPAA and Information Security training. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information System

Security r (ISSO), local Area Manager, System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

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

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

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

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

 Contractors will have access to the Area Boundary 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 Boundary 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 Wichita access must have an approved computer access request on file. The area manager, or designee, in conjunction with the area 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 Boundary?

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

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

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

8.4 Has Authorization and Accreditation (A&A) been completed for the Area Boundary?
If Yes, provide:

1. Approved
2. 30-Jun-2021
3. Authorized to Operate
4. 02-Oct-2020
5. 02-Oct-2021
6. 18-Sep-2020
7. The FIPS 199 classification of the system MODERATE.

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

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

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced Area Boundary Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access

ID	Privacy Controls
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	Area Boundary of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

_____

Area Privacy Officer, Keith Hall

_____

Area Privacy Officer, Andrew Freeman

_____

Area Information Systems Security Officer, Rolando Trevino

_____

Area Information Systems Security Officer, David Shaw

_____

Area Boundary Manager, Jason Parker

APPENDIX A – Notice

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

Applicable Notices

Site Type: VBA/VHA/NCA or Program Office	Applicable NOPPs
VHA	**Notice of Privacy Practices** **VHA Privacy and Release of Information:**
VBA	**Privacy Statement on VA Forms:** PRIVACY ACT INFORMATION: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA Programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is required to obtain or retain benefits. VA uses your SSN to identify your claim file. Providing your SSN will help ensure that your records are properly associated with your claim file. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by Federal Statute of law in effect prior to January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine maximum benefits under the law. The responses you submit are considered confidential (38 U.S.C. 5701). Information submitted is subject to verification through computer matching programs with other agencies **SOR 58VA21/22/28**
NCA	**VA Form 40-0247** **VA Form 40-1330** **VA Form 40-1330M**

APPENDIX B – PII Mapped to Components

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

PII Mapped to Components Table

Components of the Area Boundary collecting/storing PII (Each row refers to a grouping of databases associated with a single server)	Does this component collect PII? (Yes/No)	Does this component store PII? (Yes/No)	Does this component share, receive, and/or transmit PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards	Provide Names of Applicable Sites
Server 1: • Encore Pro 2 • iMedAudit • TLCHOSPICE • UpdateHistory	Yes	Yes	Yes	Patient name, SSN, DOB, and demographic data	This data is needed to facilitate patient care	Server is stored in a secured environment and managed with restricted access controls	Robert J. Dole VA Medical Center
Server 2: • EMR (Vista Read Only)	Yes	Yes	Yes	Patient name, SSN, DOB, and demographic data	This data is needed to facilitate patient care	Server is stored in a secured environment and managed with restricted access controls	Robert J. Dole VA Medical Center
Server 3: • NOAHDATABASECORE • Censis_Beta_V2_Global • Censis_Graphics • Censis_HL1572 • Censis_SG1572 • CensisBufferAgent • RightFax	**Yes**	**Yes**	**Yes**	Patient name, SSN, DOB, and demographic data	This data is needed to facilitate patient care	Server is stored in a secured environment and managed with restricted access controls	Robert J. Dole VA Medical Center

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