<u>Date PIA submitted for review:</u>

June 15, 2023

<u>Privacy Impact Assessment for the VA Boundary called[1]:</u>

Area Denver

CONTINENTAL DISTRICT

---

[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	Station Numbers
1) Eastern Colorado Health Care System (ECHCS)	554
2) Office of Integrated Veteran Care (IVC)	135
3) Veterans Benefits Administration (VBA)	339
4) 4A RCS Western Mountain Regional Office	500
5) Alamosa/San Luis Valley Clinic/Sierra Blanca Clinic	567GC
6) Aurora Community Based Outpatient Clinic (CBOC)	554GB
7) Bioscience	554
8) Boulder Vet Center	527
9) Burlington VA Outreach Clinic	554GI
10) C&P VBA Training Facility	339
11) Colorado Springs 10th Medical Group Building	554
12) Colorado Springs PFC Floyd K Linsdstrom (CBOC)	554GE
13) Colorado Springs Vet Center	525
14) Continental Memorial Service Network	789
15) Continental Regional Counsel District Office	339
16) Continental VBA District Office	384
17) Denver A Interim Data Center	554
18) Denver Combat Call Center	554CCC
19) Denver Homeless Domiciliary	554DOM
20) Denver Regional Benefit Office	789
21) Denver VA Community Resource and Referral Center (VACRRC)	554CRRC
22) Denver VA Domiciliary	554DOM
23) Denver Vet Center	504
24) Fisher House	554
25) Fort Lyon National Cemetery	889
26) Garden of the Gods Outlying Clinic	554G
27) Golden Community Based Outpatient Clinic (CBOC)	554GC
28) IDES Fort Carson	339
29) IDES USAFA	339
30) Intake Site of Buckley Space Force Base	339
31) Intake Site at Fort Carson	339
32) Intake Site at Peterson Space Force Base	339
33) Intake Site at Schriever Space Force Base	339
34) Intake Site at USAF Academy	339
35) Jewell VA Clinic	554QB
36) La Junta Community Based Outpatient Clinic (CBOC)	554GG
37) Lamar Community Based Outpatient Clinic (CBOC)	554GH
38) Pavilion Towers (OIG)	554OIG
39) Pikes Peak National Cemetery	993
40) Pueblo NHCU (CLC)	554CLC
41) Pueblo Community Based Outpatient Clinic (CBOC)	554GD
42) Pueblo Vet Center	542
43) Salida VA Telehealth Clinic	554QC
44) SAO West, NCO 19 Rocky Mtn. Acquisition Center	554SAO
45) Union Blvd Community Based Outpatient Clinic (CBOC)	554GK

46) VBA Human Resource Center Denver	339
47) VISN 19: Rocky Mountain Network	10N19
48) Vocational Rehabilitation Office – Colorado Springs	525
49) Western Public Affairs Office	554PA

Boundary Contacts:

Boundary Key Stakeholders

Name	*Title (PO, ISSO, AM, MD/SPS Staff, Facility Director)*	*Phone Number*	*Email Address*	*Applicable Site (VBA, VHA, NCA, Program Office)*
Eller Pamintuan	IVC, Privacy Officer	303-331-7512	eller.pamintuan@va.gov	VHA-IVC
Dana Krishland	ECHCS, Privacy Officer	720-723-6765	dana.krishland@va.gov	VHA ECHCS
Daniel Quigley	Privacy Officer	303-914-5875	daniel.quigley@va.gov	VBA
Cindy Merritt	Privacy Officer	321-200-7477	Cindy.merritt@va.gov	NCA
Ashton Botts	IVC, ISSO	303-398-7155	ashton.botts@va.gov	VHA-IVC
Je'Nean Clark	ECHCS, ISSO	720-434-6919	je'nean.clark@va.gov	VHA-ECHCS
Eduardo Lorenzo	ISSO	303-914-5889	eduardo.lorenzo@va.gov	VBA
Bernadette Bowen-Welch	ISSO	202-340-8970	bernadette.bowen-welch1@va.gov	NCA
Jim Hughes	Area Manager	303-331-7898	jim.hughes@va.gov	VBA / VHA / NCA

Abstract

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

Area Denver is an Information Boundary that consists of Eastern Colorado Health Care System (ECHCS), Office of Integrated Veteran Care (IVC), Veterans Benefits Administration (VBA), 4A RCS

Western Mountain Regional Office, Alamosa/San Luis Valley Clinic/Sierra Blanca Clinic, Aurora Community Based Outpatient Clinic (CBOC), Bioscience, Boulder Vet Center, Burlington VA Outreach Clinic, C&P VBA Training Facility, Colorado Springs 10th Medical Group Building, Colorado Springs PFC Floyd K Lindstrom (CBOC), Colorado Springs Vet Center, Continental Memorial Service Network, Continental Regional Counsel District Office, Continental VBA District Office, Denver A Interim Data Center, Denver Combat Call Center, Denver Homeless Domiciliary, Denver Regional Benefit Office, Denver VA Community Resource and Referral Center (VACRRC), Denver VA Domiciliary, Denver Vet Center, Fisher House, Fort Logan National Cemetery, Fort Lyon National Cemetery, Garden of the Gods Outlying Clinic, IDES Fort Carson, IDES USAFA, Intake Site at Buckley Space Force Base, Intake Site at Fort Carson, Intake Site at Peterson Space Force Base, Intake Site at USAF Academy, Jewell VA Clinic, La Junta Community Based Outpatient Clinic (CBOC), Lamar Community Based Outpatient Clinic (CBOC), Pavilion Towers (OIG), Pikes Peak National Cemetery, Pueblo NHCU (CLC), Pueblo Community Based Outpatient Clinic (CBOC), Pueblo Vet Center, Salida VA Telehealth Clinic, SAO West, NCO 19 Rocky Mtn. Acquisition Center, Union Blvd Community Based Outpatient Clinic (CBOC), VBA Human Resource Center Denver, VISN 19, Rocky Mountain Network, Vocational Rehabilitation Office – Colorado Springs, and Western Public Affairs Office. The 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 Boundary 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 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 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 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 Boundary name and the name of the sites within it.*
- *The business purpose of the Boundary and how it relates to the program office and agency mission.*
- *Whether the 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 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 Boundary.*
- *A citation of the legal authority to operate theBoundary.*
- *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 Boundary host or maintain cloud technology? If so, does the Boundary have a FedRAMP provisional or agency authorization?*

The *Area Denver* itself does not collect, use, disseminate, maintain, or store Personally Identifiable Information (PII) or Protected Health Information (PHI). VHA, VBA and NCA Facilities located within the *Area Denver* IT Boundary all access VA Enterprise IT systems respectively, hosted and maintained outside of this boundary. These are VISTA, VBMS, MEM, etc.

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

The facilities within the 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 (location 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 Boundary is using the VA Enterprise Cloud (VAEC) which is at the enterprise level and is outside of the Boundary. Further information can be found in the VAEC PIA located at https://www.oprm.va.gov/docs/PIA/FY22VAEnterpriseCloudPIA.pdf.

VHA-ECH - The General Support System (GSS), officially known as ECH-VHA-GSS, is a facility level system that operates under the authority of *Veteran's Benefits: Functions of Veterans Health Administration*, Title 38 U.S. Code, § 7301. The GSS system consist of servers, workstations, laptops, printers, Commercial off the Shelf (COTS) software, and other related applications. The system contains and transmits contact, personal health, military, and financial information on approximately 100,000 Veterans, their dependents, volunteers, employees, and contractors.

The GSS is a new system that was created mid-year 2013, when the Office of Information and Technology (OIT) made major changes to VA systems and their security boundaries. Previously ECH operated a local area network (LAN), which was then divided into this GSS and backbone support system which contains no personally identifiable data or memory capability. Consequently, all the Personally Identifiable Information (PII) and Sensitive Personal Information (SPI) that once resided on the ECH LAN now reside on the Region 1, GSS. A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example:

• LAN including smart terminals that support a branch office
• Backbone (e.g. agency-wide)
• Communications network
• Agency data processing center including its operating system and utilities
• Tactical radio network
• Shared information processing service facility

The LAN is the primary and only network supporting ECH users in their day-to day operations. The LAN is continuously used during business and non-business hours, supporting many businesses

processing across all ECH facilities in a computing environment. The confidentiality, integrity and availability of the LAN is critical, i.e., ensuring that data is only received by the persons and applications that it is indented for, that data is not subject to unauthorized or accidental alterations, and that the resources are available when needed. Due to the sensitivity of the LAN, and/or data, all VA personnel with network/system access are required to obtain appropriate background investigation clearances to fulfill their duties.

The ECH GSS conducts a variety of information sharing both internal and external to the Department of Veterans Affairs. Internal sharing, discussed in greater detail in Section 4 of this Privacy Impact Assessment (PIA), is generally done to ensure that Veterans and their families receive the benefits and care that they have earned. We share patient data with the VA Veterans Benefits Administration (VBA), VA Heath Eligibility Center (HEC), and Consolidated Patient Account Center (CPAC), in addition to other VA departments and programs. External sharing, which is discussed in greater detail in Section 5 of this PIA, is done for several reasons with the Social Security Administration, state health and Veteran's agencies in Wyoming and Nebraska, and other agencies and organizations. The following VA System of Record Notices (SORNs) applies to the General Support System: as shown in the "Applicable SORs" table below under the VHA section.

The legal authorities to operate the GSS system are Title 5, United States Code, section 301, Title 38, United States Codes, sections 109, 111, 501, 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, and 7105 and Title 38, United States Code, Section 7301 (a).

VHA-IVC - Site consists of one main campus located in Denver, CO. The system environment is comprised of workstations, laptops, portable computing devices, terminals, servers, printers, special purpose systems, and a data center. The system 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 system environment also includes as applicable, subsystem components such as tape drives, optical drives, disk drives, network area storage (NAS), storage access networks (SAN), archival appliances and tier 2 storage solutions.

The VHA-IVC site encompasses the management, operational, and technical security controls associated with IT hardware, consisting of servers, routers, switches, hubs, gateways, peripheral devices, desktop/laptops, and OS software. The Information System employs a myriad of routers and switches that connect to the VA network. Routers provide connectivity to the VA WAN and switches provide connectivity to servers and gateways. The information system is designed to provide Local Area Network (LAN), Wide Area Network (WAN) and wireless connectivity. The WAN design incorporate Core/Distribution and Access layers. WAN circuits are provisioned with redundant carriers.

VHA-IVC site operates under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, §7301(a) and Public Law 87–693; 42 U.S.C. 2651, commonly known as the *Federal Medical Care Recovery Act.*

The purpose of VHA-IVC site is to directly support the mission of providing care and to all of our Nation's Veterans and eligible beneficiaries VA offers health care and services for a Veteran's family members and dependents (beneficiaries) based on certain conditions and eligibility requirements. VA serves more than 548,429 beneficiaries through its family member and dependent health care benefit

programs. In general, these programs reimburse the costs of specific types of covered services provided. VA provides care to more than 420,000 Veterans through community providers when VA cannot provide the care needed. Community care is based on specific eligibility requirements, availability of VA care, and the needs and circumstances of individual Veterans. This care is provided on behalf of and paid for by VA.

Internal sharing, discussed in greater detail in Section 4 of this Privacy Impact Assessment (PIA), is generally done to ensure that Veterans and their families receive the benefits and care that they have earned. VHA-IVC site shares information with VA systems/applications and business associated to facilitate the payment of care in the community as authorized by the Veteran Health Administration Medical Centers. External sharing, which is discussed in greater detail in Section 5 of this PIA, is done for several reasons to facilitate and pay for care in the community.

VHA-IVC site does not employ cloud computing. The completion of the PIA will not result in business changes and the System of Records Notice (SORN) does not need to be amended. All applicable SORs for IVC are shown in "Applicable SORs" table below under the VHA section.

The legal authorities to operate the GSS system are: 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, Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq., Title 5 U.S.C 301, Title 26 U.S.C 61, Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787,1802, 1803, 1812, 1813, 1821, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.

VBA - VBA Regional Offices, under the direction of the Veterans' Benefits Act (38 U.S. Code Chapter 77), provide benefits and services to eligible Veterans, their families, and beneficiaries. These benefits and services include compensation, pension, education, insurance, loan guaranty, and vocational rehabilitation and counseling. VBA activities address the receipt, processing, tracking, and disposition of Veterans' applications for benefits, services, and requests for assistance. VBA activities also address the general administration of legislated benefit programs.

To help fulfill the responsibilities of the VBA, the Denver Regional Office uses a general support system (GSS) to assist in serving 1,000,000 to 9,999,999 Veterans and their dependents. Our GSS consists of file servers, routers, printers, and networked PCs which allow for the processing and storage of data necessary for carrying out VBA functions. The Denver Regional Office GSS does not directly host or maintain any major VA systems or applications. Any data stored on the system is the result of employees directly storing or maintaining data, such as Excel Spreadsheets or Word Documents, on the network. Although most Veteran data are stored in a central database not located at this facility, during the processing of benefits, it is often necessary for employees to store files containing personal information on the network. This is done for a variety of reasons to include but not limited to temporary storage while working a case, for reference purposes, or to assist in case management. Any potential records created, maintained, or stored on the Denver Regional Office GSS are governed by Veterans Affairs System of

Record Notice (VA SORN) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28 (July 19, 2012).

The Denver Regional VBA Office GSS connects directly to the VA Enterprise wide-area network, maintained by the VA Network Security Operations Center (NSOC). This allows select users at the Denver Veterans Affairs Medical Center (VAMC) limited access to a Web-based Hospital Inquiry database known as WebHinq and Veterans Information Solution (VIS), which are used to verify Veterans' eligibility for benefits; and Veterans Benefits Management System (VBMS), which is used to process Veterans' disability claims. Accredited co-located and remote Veterans Service Organizations, such as Colorado Division of Veterans Affairs, Disabled American Veterans, Veterans of Foreign Wars, American Legion, Military Order of Purple Heart, Paralyzed Veterans of America, etc., are provided read only access to Control of Veteran's Records (COVERS), SHARE, a Microsoft Windows®-based application which is utilized by the Regional Offices (RO) to access the Beneficiary Inquiry Records Locator System (BIRLS), Compensation and Pension (C&P) Master Records, Pending Issue File (PIF), Payment History File (PHF), Corporate database, Social Security Administration, and COVERS records. SHARE provides a single computing system with data sources located on different databases in multiple locations. Additional applications to help perform proper claims development include Veterans Appeals Control and Locator System (VACOLS), Virtual VA, and Modern Award Processing (MAP-D). No major applications are supported by this system. All the major applications are supported and located at various sites throughout the United States, and the local general support system (GSS) only accesses the applications through the network. The Denver RO GSS simply hosts the client portion of each client-server major application. The Regional Offices are a separate system from the Veterans Affairs Enterprise-Wide Area Network (VA EWAN) and are managed separately. The Veteran's claims information is either entered manually from paper submitted forms or transferred electronically from information entered through the web based eBenefits portal. The system is not a regional system. either entered manually from paper submitted forms or transferred electronically from information entered through the web based eBenefits portal. The system is not a regional system.

NCA - Provides the gravesite, grave liner, opening and closing of the grave, government headstone or marker, U.S. burial flag, Presidential Memorial Certificates, and perpetual care of the gravesite at no cost to the family.

VA operates 155 national cemeteries and 34 soldiers' lots and monument sites in 42 states and Puerto Rico. More than 4 million Americans, including Veterans of every war and conflict, are buried in VA's national cemeteries. VA also provides funding to establish, expand, improve, and maintain 121 Veterans cemeteries in 49 states and territories including tribal trust lands, Guam, and Saipan. For Veterans not buried in a VA national cemetery, VA provides headstones, markers, or medallions to commemorate their service. In 2017, VA honored more than 361,892 Veterans and their loved ones with memorial benefits in national, state, tribal and private cemeteries.

The applicable SORs for *Area Denver* include:

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	Applicable System of Records (SORs)
VHA	• Applicants for Employment under Title 38, USC-VA, SORN 02VA135 • Automated Safety Incident Surveillance and Tracking System – VA, SOR 99VA13 (March 31, 2009)

Site Type: VBA/VHA/NCA or Program Office	Applicable System of Records (SORs)
	• Community Care (CC) Provider Profile Management System (PPMS) – VA, SOR 186VA10D (January 25, 2021) • Community Placement Program – VA, SOR 65VA122 • Community Residential Care and Medical Foster Home Program – VA, SOR 142VA114 • Compliance Records, Response, and Resolution of reports of Persons Allegedly Involved in Compliance Violations – VA, SOR 106VA17 • Customer Relationship Management System (CRMS) – VA, SOR 155VA10NB (March 3, 2015) • Employee Medical File System Records (Title 38) – VA, SOR 08VAO5 • Employee Medical Files System Records – VA, SOR Title 5: OPM/GOVT-10 • Enrollment and Eligibility Records – VA, SOR 147VA10 (August 17, 2021) • Health Information Exchange - VA 168VA005 • Health Care provider credentialing and Privileging Records – VA, SOR 77VA10Q (March 26, 2008) • Health Care Provider Credentialing and Privileging Records - VA¸SOR 77VA10E2E • HealthShare Referral Manager (HSRM) – VA, SOR 180VA10D (August 17, 2021) • Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attending, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records – VA, SOR 14VA05 (November 18, 2010) • Income Verification Records – VA, SOR 89VA19 (May 8, 2008) • National Patient Databases – VA, SOR 121VA10A7 (February 12, 2018) • Non-VA Care (Fee) Records – VA, SOR 23VA10NB3 (July 30, 2015) • Patient Advocate tracking System (PATS) – VA, SOR 100VA10NS10 • Police and Security Records – VA, SOR 103VAO7B • Patient Medical Records – VA, SOR 24VA10A7 (October 2, 2020) • Telephone Service for Clinical Care Records – VA, SOR 113VA112 (May 8, 2009 • The Revenue Program-Billing and Collections Records – VA, SOR 114VA10 (January 25, 2021) • Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA, SOR 54VA10NB3 (March 3, 2015) • Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SOR 79VA10 (December 23, 2020) • Veteran, Patient, Employee, and Volunteer Research and Development Project Records – VA, SOR 34VA12 (May 27, 2010) • Veterans, Service Members, Family Members, and VA Beneficiary Survey Records – VA, SOR 43VA008 • VHA Corporate Data Warehouse – VA, SOR 172VA10 (December 22, 2021)

Site Type: VBA/VHA/NCA or Program Office	Applicable System of Records (SORs)
VBA	• Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA, SOR 58VA21/22/28 (November 8, 2021)
NCA	• VA National Cemetery Pre-Need Eligibility Determination Records – VA, SOR 175VA41A • Veterans and Dependents National Cemetery Gravesite Reservation Records – VA, SOR 41VA41 • Veterans and Dependents National Cemetery Interment Records – VA, SOR 42VA41 • Veterans (Deceased) Headstone or Marker Records – VA, SOR 48VA40B

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, Boundary, or technology being developed.

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

Identify and list all PII/PHI that is collected and stored in the Boundary, including Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series. If the Boundary creates information (for example, a score, analysis, or report), list the information the Boundary is responsible for creating.

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

Please check any information listed below that the facilities within the 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 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
☒ Requestor Information
☒ Death Certification Information
☒ Criminal Background Information
☒ Education Information
☒ Gender
☒ Tumor PHI Statistics

☒ Other Unique Identifying Information (list below)
- Age
- Benefit Information
- Biometrics
- Burial Service
- Date of Service
- Demographics
- Dental Eligibility
- Eligibility Date
- Funeral Information
- Headstone data
- Internal Control Number
- International Code Designator (ICD), diagnosis codes

- Marital Status
- Member ID
- Other Health Insurance (OHI)
- Place of Burial
- Place of Service
- Referral
- Relationship to Veteran
- Rendering Provider Zip Code
- Social Work Assessment
- VA Employee Name
- VA Login Identification (ID)

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

PII Mapping of Components (Servers/Database)

Area Denver consists of **23** 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 Denver* 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 Boundary?

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

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

The information that resides within the facilities in the 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 46VAA00, 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
- Identity and Access Management (IAM) Single Sign-On Internal (SSOi) and User
- Provisioning: Memorial Benefits Management System (MBMS) Salesforce and Amazon Web Services (AWS) uses two VA IAM services to validate user login information: SSOi and User Provisioning.
- Veterans Benefits Management System (VBMS) eFolder via iHub: Provides access to a widget allowing National Cemetery Scheduling Office (NCSO) case managers the ability to view documents in eFolder to assist in eligibility verification of Veterans and Next-of-Kin.
- The data viewed is viewed for eligibility determinations and not transmitted or stored in MBMS Salesforce or AWS.
- VA Master Persons Index Enterprise (MPIe): Provides the ability to search the authoritative data source for Veterans, MPI, to ensure that they are not creating duplicate contact records in applications built on the Salesforce platform.
- Direct conversation with individual Veterans or NOK who call the NCSO representatives

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

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

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. Claim forms submitted to VHA by community providers for payment.
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 https://www.va.gov/find-forms/. The URL of the associated privacy statement is https://www.oprm.va.gov/. 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.
NCA	MEM does receive information electronically from other systems, such as Veterans Benefits Management System (VBMS) eFolder via iHub, Identity and Access Management (IAM) Single Sign-On Internal (SSOi) and User Provisioning, VA Master Persons Index Enterprise (MPIe), and direct conversation with individual Veterans or Next of Kin. Information is received, reviewed, and collected through inbound and outbound telephone engagement, in-person contact, postal mail, and fax, to the National Cemetery Scheduling Office (NCSO), Applicant Assistance Unit (AAU), national cemeteries, and other NCA offices.

Site Type: VBA/VHA/NCA or Program Office	Means of Collection
	Data is manually entered into all NCA systems except for the Enterprise Eligibility Office Automation System (EOAS). EOAS receives applications and documents via direct upload from VA.gov. Forms and supporting documentation required to verify memorial benefits eligibility, such as the DD-214, are scanned/uploaded into the document repositories such as FEITH, EOAS, and eFolder and stored in the Memorial Data Warehouse. AMAS processes approximately 360,000 claims for standard government headstones or markers (VA Form 40-1330) and Monument and Presidential Memorial Certificate Request (VA Form 40-0247) applications annually. Data from the forms are manually entered into the system. Forms and supporting documentation required to verify memorial benefits eligibility, such as the DD214, are scanned/uploaded.

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 Denver* using several methods, to include site-to-site connection, facsimile, mail and/or email. 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.

NCA: The Memorial Benefits Management System (MBMS) is under development to replace the BOSS-E and AMAS system suite. MBMS has replaced BOSS-E as the primary scheduling tool at the NCSO and will replace all NCA systems to include BOSS, AMAS, EOAS, Web-Presidential Memorial Certificates (Web-PMC), and Memorial Enterprise Letters (MEL) by 2025.

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

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

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

Site Type: VBA/VHA/NCA or Program Office	Purpose of Information Collection
NCA	• MEM collects and maintains information to verify the identity and eligibility of the Veteran or decedent for burial and monument services

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

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

*[Review the suggested answer below and list any other procedures used by this boundary to check information for accuracy. **Please remember processes at this boundary may differ from the standardized answer below**].*

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.

VHA: - 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. Some information collected from the public, including income information and military service history, are verified

against information provided by other U.S. Agencies – the Internal Revenue Service (IRS) and Social Security Administration (SSA) for income information and the DoD for military history by automated tools with connections to the Austin Automation Center are obtained.

NCA: - Standard operating procedures (SOPs) are in place at NCA offices and cemeteries to perform quality control on data related to each case. As cases progress through the queues from NCSO case managers to the cemetery office staff, additional data integrity checks are conducted. Final data integrity checks are performed by cemetery operations staff who perform the interment after services.

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

List the full legal authority for operating the Boundary, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.

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

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 VA Cyber Security Program. • Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (February 17, 2009), codified at 42 USC. §§300jj et seq.; §§17901 et seq. • Title 5 USC 301 • Title 26 USC 61 • Title 38, USC. Sections 31, 109, 111, 501, 1151, 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741-1743, 1781, 1786, 1787, 1802, 1803, 1812, 1813, 1821, 3102, 5701(b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131-8137. • 38 Code of Federal Regulations (CFR) 2.6. • 45 CFR, Part 1610 and 164 • Title 44 USC and Title 45 USC, Veterans Access, Choice, and Accountability Act of 2014 • Public Law 103-446, Section 107 • Public Law 111-163, Section 101
VBA	• Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b) • Authority to operate the Veteran Benefit Administration comes from 38 U.S. Code Chapter 77 • Specific authority to operate the Denver Regional Office General Support System (GSS) is Title 10 U.S.C. Chapters 106a, and 10, and Title 38, U.S.C. Section 501(1) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, and 55. This information is reflected in the VA SORN Compensation, Pension, Education and Vocational Rehabilitation and Employment Records – VA, SORN 58VA21/22/28 (Jul 19, 2012). The legal authority to use and collect Veteran social security numbers comes from 38 CFR 3.216; 38 CFR 1.575(b); 38 CFR 14.631; 38 USC 5101(c); 38 U.S. Code 7703; Title 5 USC 522a(a)(4).1.575(b)
NCA	• National Cemetery, Title 38, United States Code (U.S.C.) Chapter 38 § 101, 38 CFR Subpart B , 38 CFR 3.1700-CFR

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 VA Cyber Security Program. • Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (February 17, 2009), codified at 42 USC. §§300jj et seq.; §§17901 et seq. • Title 5 USC 301 • Title 26 USC 61 • Title 38, USC. Sections 31, 109, 111, 501, 1151, 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741-1743, 1781, 1786, 1787, 1802, 1803, 1812, 1813, 1821, 3102, 5701(b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131-8137. • 38 Code of Federal Regulations (CFR) 2.6. • 45 CFR, Part 1610 and 164 • Title 44 USC and Title 45 USC, Veterans Access, Choice, and Accountability Act of 2014 • Public Law 103-446, Section 107 • Public Law 111-163, Section 101
	3.1713. Amended By Public Law No. 104---231, 110 Stat. 3048 • 5 U.S.C. § 552a, Privacy Act of 1974, As Amended • 48VA40B – Veterans (Deceased) Headstone or Marker Records-VA, per Title 38, United States Code: Sections 501(a), 501(b), and Chapter 24, Sections 2400-2404. • Public Law 100---503, Computer Matching and Privacy Act of 1988 • Privacy Act of 1974; U.S Code title 5 USC section 301 title 38 section 1705, 1717, 2306-2308 & Title38, US Code section 7301 (a) and Executive Order 9397 • OMB Circular A---130, Management of Federal Information Resources, 1996 • OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites • OMB Memo M---99---18, Privacy Policies on Federal Web Sites • OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions

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 VA Cyber Security Program. • Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (February 17, 2009), codified at 42 USC. §§300jj et seq.; §§17901 et seq. • Title 5 USC 301 • Title 26 USC 61 • Title 38, USC. Sections 31, 109, 111, 501, 1151, 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741-1743, 1781, 1786, 1787, 1802, 1803, 1812, 1813, 1821, 3102, 5701(b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131-8137. • 38 Code of Federal Regulations (CFR) 2.6. • 45 CFR, Part 1610 and 164 • Title 44 USC and Title 45 USC, Veterans Access, Choice, and Accountability Act of 2014 • Public Law 103-446, Section 107 • Public Law 111-163, Section 101
	• OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII • State Privacy Laws • The legal authority is 38 U.S.C 7601-7604 and U.S.C 7681-7683 and Executive Order 9397

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 Denver* 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 Denver* 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 boundary 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 Boundary will be used in support of the program's business purpose.

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

- **Name**: Used to identify the patient during appointments and in other forms of communication
- **Social Security Number**: Used as a patient identifier and as a resource for verifying income Information with the Social Security Administration
- **Date of Birth**: Used to identify age and confirm patient identity
- **Mother's Maiden Name:** Used to confirm patient identity
- **Mailing Address**: Used for communication, billing purposes and calculate travel pay
- **Zip Code**: Used for communication, billing purposes, and to calculate travel pay
- **Phone Number(s):** Used for communication, confirmation of appointments and conduct Telehealth appointments
- **Fax Number**: used to send forms of communication and records to business contacts, Insurance companies and health care providers
- **Email Address**: used for communication and MyHealtheVet secure communications
- **Emergency Contact Information (Name, Phone Number, etc. of a different individual):** Used in cases of emergent situations such as medical emergencies.
- **Financial Account Information:** Used to calculate co-payments and VA health care benefit eligibility
- **Health Insurance Beneficiary Account Numbers**: Used to communicate and bill third part Health care plans
- **Certificate/License numbers**: Used to track and verify legal authority to practice medicine and Licensure for health care workers in an area of expertise.
- **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 Boundary sift through large amounts of information in response to a user inquiry or programmed functions. Facilities may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some facilities perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis facilities within the Boundary conduct and the data that is created from the analysis.

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

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

The VA *Area Denver* 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?

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 Boundary controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

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

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

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

The controls in place to assure 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 Boundary?

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

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

The *Area Denver* itself, does not retain information.

- Age

- Benefit Information
- Biometrics
- Burial Service
- Certificate/License number
- Criminal background information
- Current Medications
- Date of Birth
- Date of Service
- Death certificate information
- Demographics
- Dental Eligibility
- Education Information
- Electronic Protected Health Information (ePHI)
- Eligibility Date
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Employment information
- Financial Account Information
- Funeral Information
- Gender
- Guardian Information
- Headstone data
- Health Insurance Beneficiary Account Numbers
- Internal control Number
- International Code Designator (ICD), diagnosis codes
- Internet Protocol (IP) Address Numbers
- Marital Status
- Medical Record Number
- Member ID
- Military history/service connection
- Mother's Maiden Name
- Name
- Next of Kin
- Other Health Insurance (OHI)
- Personal Email address
- Personal Fax Number
- Personal Mailing Address
- Personal Phone Number(s)
- Place of Burial
- Place of Service
- Previous Medical Records
- Race/Ethnicity
- Referral
- Relationship to Veteran
- Rendering Provider Zip Code
- Requester Information
- Service-connected disabilities

- Social Security Number
- Social Work Assessment
- Tax Identification Number (TIN)
- Tumor PII/PHI statistics
- VA Login Identification (ID)
- Veteran dependent information

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 Boundary may have a different retention period than medical records or education records held within your Boundary, please be sure to list each of these retention periods.
The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

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

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. - Claim records are retained for 6 years after all individuals in the record become ineligible for program benefits. Record Control Schedule (RCS) 10-1, Chapter one- 1260- Civilian Health and Medical Care Program. VHA RCS 10-1 4000- Financial Management and Reporting Records, 4000.1b: Financial Transaction Records Related to Procuring Goods

Site Type: VBA/VHA/NCA or Program Office	Length of Retention
	and Services, Paying Bills, Collecting Debts, and Accounting. Temporary, Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.
VBA	• Compensation, pension, and vocational rehabilitation claims folders are retained at the servicing regional office until they are inactive for three years, after which they are transferred to the Records Management Center (RMC) for the life of the Veteran. • Official legal documents (e.g., birth certificates, marriage licenses) are returned to the claimant after copies are made for the claimant's file. At the death of the Veteran, these records are sent to the Federal Records Center (FRC) and maintained by the National Archives and Records Administration (NARA) in accordance with NARA policy. • Once a file is electronically imaged and accepted by VBA, its paper contents (with the exception of documents that are the official property of the Department of Defense, and official legal documents), are destroyed in accordance with Records Control Schedule VB–1 Part 1 Section XIII, as authorized by NARA. • Documents that are the property of the Department of Defense are either stored at the RMC or transferred to NARA and maintained in accordance with NARA policy. • Vocational Rehabilitation counseling records are maintained until the exhaustion of a Veteran's maximum entitlement or upon the exceeding of a Veteran's delimiting date of eligibility (generally, ten or twelve years from discharge or release from active duty), whichever occurs first, and then destroyed. • Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and 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.
NCA	• Veterans (Deceased) Headstone or Marker Records-VA SORN 48VA40B: Retained indefinitely • NCA RCS

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

Retention Schedule Table

Site Type: VBA/VHA/NCA or Program Office	Retention Schedule
VHA	Department of Veteran Affairs Records Control Schedule 10-1 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf) Department of Veteran Affair, Office of Information & Technology (OI&T) Records Control Schedule 005-1 (https://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf)
VBA	https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc
NCA	48VA40B, Veterans (Deceased) Headstone or Marker Records – VA (https://www.govinfo.gov/content/pkg/FR-2010-10-21/pdf/2010-26490.pdf) Retained indefinitely NCA RCS

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 Denver** 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)

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) (https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1254&FType=2)**. 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 Boundary include any facility or program that, where feasible, uses techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

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

VHA-ECH - No PII is used to test systems prior to deployment. All testing is conducted with test samples of the required application categorization of the subject.

VHA-IVC -
- Training: Call Center representative live training
- Research: Site does not conduct research

VBA - The Denver Regional Office does not conduct research or testing activities. Locally developed presentations for training purposes, that may become publicly available, do not contain PII per VA Directive 6511, and are reviewed by the Denver Regional Office Privacy Officer and certified via VA Form 0897, Presenter Certification.

Training is also conducted locally for Veterans Service Center (VSC) employees with oversight from VBA's Compensation Service Training. Type of data used by VBA include limited data sets, with mock information (no live claim data) or de-identified information, with all PII removed. This training utilizes approved and controlled access to the Veterans Benefits Management System (VBMS) in "Demonstration Mode", which contain dummy information and is not connected to live claims information. Additionally, live claims information is not presented in recorded environments; PII is not exposed to non-VA personnel. Al training access is documented using controlled access with a unique student number and pseudo-claim number assigned.

NCA - PII collected by MEM is not used for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information
Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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 Boundary.

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

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

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

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

Privacy Risk: There is a risk that the information maintained by *Area Denver* 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 Denver* 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 Denver* 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 boundary 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.

VBA Mitigation: Paper records are shredded on a weekly basis. Shredding is conducted on site. The Denver Regional Office uses a GSA contracted provider, Truss Crane, Inc. DBA all American Records Management. Truss Crane Inc. holds a contract through GSA for the Denver metropolitan area. The Denver Regional Office keeps certificates of destruction on file for Truss Crane's services. VBA Letter 20-08-63 is followed regarding Shredding Service Contracts. All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness and Rules of Behavior training annually. The Denver Regional Office adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).

NCA: File plans are created by each individual office/facility, according to NCA RCS and GRS. File plans are updated and inventoried annually or as needed for business.

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 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 Boundary 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 Boundary within VA with which information is shared.

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

For each interface with a system outside each facility, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.
Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

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

Data Shared internally by facilities within the Boundary 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*	*Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)*
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	VBA
Veterans Health Administration (VistA)	Electronic Health Record	System Log files, sample clinical data that may contain Protected Health Information (PHI)	Electronically pulled from VistA thru Computerized Patient Record System (CPRS)	VBA
Veteran Health Administration (VHA)	Determine eligibility for	Name: Social Security Number: Date of Birth: Mailing Address: Zip	Electronic transmission	VBA

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 Boundary (VBA, VHA, NCA, Program Office)
	Veteran compensation	Code: Phone Numbers: Email Address: Emergency Contact Information: Financial Account Information: Health Insurance Beneficiary Numbers Current Medications: Previous Medical Records:	methods in accordance with VA policy. Paper records are shared with the VHA to conduct medical examinations to determine Veteran's eligibility for compensation. The VHA accesses Veteran's information in VBMS and VIS to verify eligibility.	
Veteran Health Administration	Active Directory Service Accounts	VA Contractors: name, personal mailing address, personal phone number (s)	VA Network	VHA-HAC-IVC
Veteran Health Administration	Attachments Retrieval System	Name, social Security Number, date of birth, mailing address, zip code, phone numbers, emergency contact information, health insurance (beneficiary numbers, account numbers), current medications, previous medical records, race/ethnicity, electronic data interchange personal identifier (EDIPI), gender, beneficiary type, contact notes, preauthorization, service-connected disability	Via a representational state transfer Web service over Hypertext Transfer Protocol Secure (HTTPS	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)
Veteran Health Administration	Central Fee System	Name, Social Security Number (SSN), Member Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and International Code Designator (ICD), Coded Billing Information, Health Information, Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.	Via secure file transfer protocol within the VA network, FIPS 2.0; CCRS: Secure data transfer via Windows file share using a drop zone behind the VA firewall, with subsequent, secure Extract Transform Load (ETL) Integration of data into CCRS.	VHA-IVC
Veteran Health Administration	Central Server (CS),	Name, Social Security Number (SSN), Date of Birth (DOB), Address, Zip Code Health Insurance Numbers, International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address,	Electronically pulled and pushed. Electronically pulled and pushed. Secure FTPS FIPS 140-2 Secure Transmission VIA VA network	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)
		Provider Remit to Address		
Veteran Health Administration	Claims Processing and Eligibility (CP&E)	Claims status, Payments, eligibility, Social Security Number (SSN); FBCS: patient and medical services data, Name, Social Security Number (SSN), Date of Birth (DOB), Address, Zip Code Health Insurance Numbers, International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address	FM CRM application. Remote procedure call to return some CP&E data. UI screen hosting for remaining CP&E data; COMMCARE: Secure login via CommCare application. Remote procedure call to return some CP&E data. User Interface (UI) screen hosting for remaining CP&E data; FBCS: A Windows service secured Architecture Design Overview (ADO) connection to Health Administration Center (HAC) SQL database	VHA-IVC
Veterans Health Administration	Computerized Patient Record System (CPRS)	Social Security Number	CPRS uses the Auto Hotkey feature provided by Consult Toolbox to send	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)
			the SSN via webAPI	
Veterans Health Administration	Corporate Data Warehouse (CDW)	Patient's Internal Control Number (ICN), Name, Email, CAN Score/Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Emergency Contact, Information, Health Insurance (Beneficiary Numbers, Account Numbers), Current Medications, Previous Medical Records, Race/Ethnicity, EDIPI, Gender Beneficiary Type (whether the individual is a Veteran or spouse of a Veteran) Contact Notes (additional information regarding, contacting the patient) Preauthorization, Service-Connected Disability, email address, Tax Identification Number (TIN), Member Identification (ID)	webAPI, web, SSIS, data adapter (varies)/ Data is sent to CDW from the various Structured Query Language (SQL) databases using HTTPS 8; EPRS: Secure VA Network (HTTPS or TLS) Azure Express Route (AER) (encrypted) VAEC Trusted Internet Connections (TIC)	VHA-IVC
Veterans Health Administration	Customer Relation Management (CRM)	Patient's ICN, Name, CAN Score/Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Emergency Contact, Information, Health Insurance (Beneficiary Numbers, Account Numbers), Current Medications, Previous Medical Records, Race/Ethnicity,	Agent Electronically enters information related the customers call.	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)
		EDIPI, Gender Beneficiary Type (whether the individual is a Veteran or spouse of a Veteran) Contact Notes (additional information regarding, contacting the patient) Preauthorization, Service-Connected Disability, email address, Tax Identification Number (TIN), Member Identification (ID).		
Veterans Health Administration	Document and Process Enabled Repositories (DAPER)	Names, Addresses, zip code, phone numbers, fax numbers, email addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, and date of Birth (DOB)	Workflow system. Information is attached to a ticket in PCDUO and assigned to a team for review.	VHA-IVC
Veterans Health Administration	Electronic Data Interchange (EDI)	Name, Social Security Number (SSN), Member Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and International Code Designator (ICD), Coded Billing Information, Health Information, Prescription Information, Procedure Codes Number, Veteran and	Via secure file Transfer protocol within the VA network, FIPS 2.0; EPRS: Secure VA Network (HTTPS or TLS) Azure Express Route (AER) (encrypted) VAEC Trusted Internet Connections (TIC)	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)
		Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary, financial account information, certificate and license numbers, previous medical records, medical record number, member identification (ID)		
Veterans Health Administration	Electronic Data Interchange (EDI) Gateway	Name, Social Security Number (SSN), Date of Birth (DOB), Address, Zip Code Health Insurance Numbers, CPY and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address	Electronically pulled and pushed. Secure FTPS FIPS 140-2 Secure Transmission VIA VA network	VHA-IVC
Veterans Health Administration	Electronic Web Viewer (EWV)	Name, Social Security Number (SSN), Date of Birth (DOB), Address, Zip Code Health Insurance Numbers, International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance	Electronically pulled and pushed. Secure FTPS FIPS 140-2 Secure Transmission VIA VA network	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)
		Information, Other Health Insurance Paid Amounts, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address		
Veterans Health Administration	Eligibility and Enrollment System (E&E)	Enrollment information for Individuals, Sensitivity Determination, Addresses, Contact Information, Eligibility Status, Enrollment Status Insurance Information	Accessed via a SOAP Web service over HTTPS; Encrypted electronic transmission (web service)	VHA-IVC
Veterans Health Administration	Enrollment & Eligibility (E&E) Webservice	Residential Address, Urgent Care Eligibility, Community Care Eligibility	Electronically pulled through E&E Web Service data interface over TLS	VHA-IVC
Veterans Health Administration	Fee Basis Claims System (FBCS)	Name, Social Security Number (SSN), Member Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and International Code Designator (ICD), Coded Billing Information, Health Information, Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number	Via secure file transfer protocol within the VA network, FIPS 2.0	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)
		(TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.		
Veterans Health Administration	Fee Payment Processing System (FPPS)	Name, Social Security Number (SSN), Member Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and International Code Designator (ICD), Coded Billing Information, Health Information, Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.	Via secure file transfer protocol within the VA network, FIPS 2.0	VHA-IVC
Veteran Health Administration	HAC VistA Outpatient Pharmacy Package	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number, Fax Number, Email Address, Health Insurance Beneficiary Numbers, Account Numbers, Certificate/License numbers, Current	No VA network connection, VA employee Query	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)
		Medications, Previous Medical Records		
Veteran Health Administration	HAC VistA Patient File	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number, Fax Number, Email Address, Health Insurance Beneficiary Numbers, Account Numbers, Certificate/License numbers, Current Medications, Previous Medical Records	No VA networks connection, VA employee Query	VHA-IVC
Veteran Health Administration Office of Community Care -Health Administration Center (HAC) all Veteran Affairs (VA) Medical Centers	Health Care Claims Processing Eligibility and Enrollment Service (HCP EE)	Patient specific SPI	Simple Object Access Protocol (SOAP) Secured SOAP synchronous XML exchange to webservice.	VHA-IVC
Veteran Health Administration	Health Data Repository (HDR)	VistA Consults, VistA Appointments, VistA Notes, VistA Postings, VistA Orders	Encrypted electronic transmission (web service)	VHA-IVC
Veteran Health Administration	Identity and Access Management (IAM) SSOe	Authentication information as provided by SSOe	SAML assertion passed as part of a redirect to our page CCRA consumes the info, SSOe provides	VHA-IVC
Veteran Health Administration	Identity and Access Management (IAM) SSOi	Authentication information as provided by SSOi	Security Assertion Markup Language (SAML)	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)*
			assertion passed as part of a redirect to our page CCRA consumes the info, SSOi provides	
Veteran Health Administration	Master Veteran Index (MVI)	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Emergency Contact, Information, Health Insurance (Beneficiary Numbers, Account Numbers), Current Medications, Previous Medical Records, Race/Ethnicity, Electronic Data Interchange Personal Identifier (EDIPI, Gender Beneficiary Type (whether the individual is a Veteran or spouse of a Veteran) Contact Notes (additional information regarding, contacting the patient) Preauthorization, Service-Connected Disability, gender	Via a Simple Object Access Protocol (SOAP) Web service over HTTPS; COMMCARE: Compensation and Pension Record Interchange (CAPRI) electronic software package; DST: Electronically sent to Master Veteran index data interface over TLS	VHA-IVC
Veteran Health Administration	VA Organizational Employees	Name, Social Security Number (SSN), Date of Birth (DOB), Address, Zip Code Health Insurance Numbers, CPY and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health	Secure log-in through OCC developed application (FPPS) Austin Automation Center to Submit Payment to Treasury	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)
		Insurance Paid Amounts, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address		
Veteran Health Administration	Program Tracking (PT)	Name, Social Security Number (SSN), Date of Birth (DOB), Address, Zip Code Health Insurance Numbers, CPY and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Provider Name, Provider Phone Number, Provider Billing address, Provider Physical Address, Provider Remit to Address	Electronically pulled and pushed. Electronically pulled and pushed. Secure FTPS FIPS 140-2 Secure Transmission VIA VA network	VHA-IVC
Veteran Health Administration	Provider Profile Management System (PPMS)	Provider National Provider Identifier (NPI), Community Care Network (CCN) Identification Number (ID), Date of Service	Via a representational state transfer Web service over Hypertext Transfer Protocol Secure (HTTPS), CCRA consumes the information PPMS Provides, CCRS Secure data transfer via OData service data share using	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)
			a service zone behind the VA firewall.	
Veteran Health Administration	Right Fax	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number, Fax Number, Email Address	Fax and the ePrescribing contract.	VHA-IVC
Veteran Health Administration	Standardized Episodes of Care (SEOC)	SEOC data, with associated treatment codes (this is not associated to Veterans or referrals at transmit time)	SEOCs will be retrieved from a SharePoint site via HTTPS	VHA-IVC
Veteran Health Administration	Workforce Optimization/Avaya Call Recorder	Name, SSN, Health Insurance Beneficiary Number, DOB, Zip Code, Health Insurance Numbers, CPY and international Code Designator (ICD) Coded Billing Information, Billed Amounts, Income Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address	Local Area Network via client on CSR's Desktop	VHA-IVC
Veteran Health Administration	Death/burial benefit	Death certificates, Veteran eligibility	Hard copy mailing	VHA-ECHCS
Veterans Benefits Administration	VBA	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	Compensation and Pension Record Interchange (CAPRI) electronic	VHA-IVC / VHA-ECHCS

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 Boundary (VBA, VHA, NCA, Program Office)
			software package	
Veteran Health Administration	VHA	System Log files, sample clinical data that may contain Protected Health Information (PHI) appropriate to the agreements	Electronically pulled from VistA thru Computerized Patient Record System (CPRS)	VHA-ECHCS
VBA – listed in PTA	Health PHI/PII pertinent to Veterans and benefits	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	Control access to VA and databases & technology systems	VHA-ECHCS
Data Access Services (DAS) – listed in PTA	Health PHI/PII pertinent to Veterans and benefits	Personally Identifiable Information (PII), Protected Health Information (PHI), Individually Identifiable Information (III), System Log files, sample clinical data that may contain Protected Health Information (PHI)	SOAP over HTTPS using SSL encryption and Certificate exchange	VHA-ECHCS
Denver VAMC's Veteran Centers	VHA	Personally Identifiable Information (PII), Protected Health Information (PHI), Individually Identifiable Information (III), System Log files, sample clinical data that may contain Protected Health Information (PHI)	Electronically reviewed through Computerized Patient Record System (CPRS)	VHA-ECHCS
VA Tumor Register	Tracking & trending of disease	Diagnosis & procedures, tumor status, treatment outcome, survivor tracking, type of treatments, demographics, hormone, radiation, chemotherapy, problem lists	Electronic tumor register package	VHA-ECHCS

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 Boundary (VBA, VHA, NCA, Program Office)
VA Network Authorization Office – Non-VA care Coordination.	Health/medical payment authorization	Demographics, diagnoses, medical history, service connection, Provider orders, VHA recommendation/approval for non-VA care	Fee Basis Claim System (FBCS) authorization software system	VHA-ECHCS
VA Health Eligibility Center	Determine Veteran eligibility	Service dates, SSAN, demographics, service connection	Scanned documents uploaded into shared software programs	VHA-ECHCS
Central Consolidated Patient Account Center (CCPAC)	Medical care cost recovery	Diagnosis, service connection, dates of service, health insurance information, demographics	Electronically pulled from VistA through Computerized Patient Record System (CPRS); Huron system extracts data from system.	VHA-ECHCS
Veteran Health Information Exchange (VHIE) a.k.a. Virtual Lifetime Electronic Record (VLER)	Health information exchange	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), Individually Identifiable Information (III), System Log files, sample clinical data that may contain Protected Health Information (PHI)	Business Partner Gateway	VHA-ECHCS
Veterans Choice Program (Veterans Access, Choice and Accountability Act of 2014)	Tracking & trending of disease progression	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) appropriate to the agreement.	secure web portal	VHA-ECHCS
National Cemetery	Memorial Benefits Management	Benefits, decedent, claimant, requestor, and	Information may be	National cemeteries and

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 Boundary (VBA, VHA, NCA, Program Office)
Administration (NCA)	System (MBMS), Burial Operations Support System (BOSS), Automated Monument Application System (AMAS), Management and Decision Support System (MADSS), Eligibility Office Automation System (EOAS), Presidential Memorial Certificate System (PMCS), Veterans Benefits Management System (VBMS), Master Person Index (MPI)	beneficiary information. Names, addresses, social security numbers, SSN, DOB, Address, Race/Ethnicity, personal representative/funeral home	transmitted upon request in a written or verbal format based on the individual request, electronically shared via network connections.	other NCA offices, as needed for processing.
VA Master Persons Index (MPI) Enterprise (MPIe)	To have the ability to search the authoritative data source for Veterans, MPI, to ensure that they are not creating duplicate contact records in applications built on the Salesforce platform	First Name, Middle Name, Last Name, Social Security Number (SSN), Date of Birth (DOB), Gender, Phone Number, Place of Birth (POB) City, Place of Birth (POB) State, Mother's Maiden Name	REST Web Service API (HTTP)	National cemeteries and other NCA offices, as needed for processing.
Burial Operations Support System Enterprise (BOSS-E)	To support legacy users	Memorial Information, Birth Date, Email, Name, Gender, Address, Date of Death, Marital Status, Military Honors, Relationship to Veteran, SSN, Phone, Country, Military Service Release from Active Duty (RAD)	Secure Database Connection – Oracle Forms based application backed by an Oracle 12c database	National cemeteries and other NCA offices, as needed for processing.

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 Boundary (VBA, VHA, NCA, Program Office)
		Date, Veteran's Period of Service, and Veteran's War Period.		
Identity and Access Management (IAM)	User access control	PII – Identity Access Information for Users access control: Name, Address, SSN (Data Encrypted)	REST Web Service API (HTTP)	National cemeteries and other NCA offices, as needed for processing.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Privacy Risk: The internal sharing of data is necessary individuals to receive benefits at the *Area Denver*. 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 Boundary 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 Boundary outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

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

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

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

Data Shared with External Organizations

List External Program Office or IT 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 Boundary (VBA, VHA, NCA, Program Office)*
SHARE Social Security Administration (SSA)	Eligibility for Federal benefits	SSN, Name, Address	National ISA/ MOU	Site to Site (S2S), IPSEC Tunnel, Secure FTP	VBA / VHA-IVC / VHA-ECHCS
Internal Revenue Services (IRS)	Income verification	Name, Financial Information	ISA/ MOU, Computer Matching Agreement	Secure Web-Portal, Secure Socket Layer	VBA / VHA-IVC / VHA-ECHCS

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 Boundary (VBA, VHA, NCA, Program Office)*
DPRIS Department of Defense	Determine military service dates, eligibility	Name, Service Information, SSN	MOU	Bi-directional Health Information Exchange	VBA
Change Health Care - Contractor Change Health (CH) - Health Care Clearing House (HCCH)	Health Care clearing house services, data storage	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Emergency Contact, Information, Health Insurance (Beneficiary Numbers, Account Numbers), Current Medications, Previous Medical Records, Race/Ethnicity, EDIPI, Gender, Beneficiary Type (whether the individual is a Veteran or spouse of a Veteran), Contact Notes (additional information regarding, contacting the patient), Preauthorization, Service-Connected Disability	Business Associate Agreement (BAA), Memorandum of understanding/ Interconnection Security Agreement (MOU/ISA)	Secure FTP	VHA-IVC
Cognosante Military Veteran Health (MVH), Limited Liability Company (LLC) - HSRM COTS	data management, information technology and support services for home telehealth platforms	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Emergency Contact, Information, Health Insurance (Beneficiary Numbers, Account Numbers),	Contract, BAA, ISA/MOU	Data is shared with external providers via HTTPS, Data includes the minimum information specific to the referral	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)*
		Current Medications, Previous Medical Records, Race/Ethnicity, EDIPI, Gender, Beneficiary Type (whether the individual is a Veteran or spouse of a Veteran), Contact Notes (additional information regarding, contacting the patient), Preauthorization, Service-Connected Disability			
Amazon Web Service (AWS) GovCloud - AWS GovCloud	Data is shared with external providers via HTTPS, Data includes the minimum information specific to the referral	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Emergency Contact, Information, Health Insurance (Beneficiary Numbers, Account Numbers), Current Medications, Previous Medical Records, Race/Ethnicity, EDIPI, Gender, Beneficiary Type (whether the individual is a Veteran or spouse of a Veteran), Contact Notes (additional information regarding, contacting the patient), Preauthorization,	Business Associate Agreement (BAA)	TIC-VPN	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)
		Service-Connected Disability			
TriWest - TriWest (contractor)	Patient centered community care, community health care coordination	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Emergency Contact, Information, Health Insurance (Beneficiary Numbers, Account Numbers), Current Medications, Previous Medical Records, Race/Ethnicity, EDIPI, Gender, Beneficiary Type (whether the individual is a Veteran or spouse of a Veteran), Contact Notes (additional information regarding, contacting the patient), Preauthorization, Service-Connected Disability	Contract and BAA	Via a representational state transfer Web service over HTTPS, CCRA consumes the information TriWest Provides; TLS, SFTP, Azure Express Route (encrypted)	VHA-IVC
Cerner - Department of Defense (DoD), Veterans Health Administration (VHA)	Software application management, remote hosting, training, and professional services	Veteran Name, Residential Address, Social Security Number (SSN), Date of Birth, Urgent Care Eligible, Community Care Eligibility, Clinical Service, Drive Time Standard, Wait Time standard, standardized episode of care	Contract, MOU, MOA, ISA	Secure Web-Portal, Secure Socket Layer SSL/TLS	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)*
		(SEOC), SEOC Description, Facility Name, Average Wait Time, Average Drive Time, Electronic Data Interchange Personal Identifier (EDIPI)			
Optum - Optum (Contractor)	patient centered community care, community health care coordination	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Emergency Contact, Information, Health Insurance (Beneficiary Numbers, Account Numbers), Current Medications, Previous Medical Records, Race/Ethnicity, EDIPI, Gender, Beneficiary Type (whether the individual is a Veteran or spouse of a Veteran), Contact Notes (additional information regarding, contacting the patient), Preauthorization, Service-Connected Disability	Contract	HL7 messages from VistA; TLS, SFTP, Azure Express Route (encrypted)	VHA-IVC
Office of Finance - Financial Management System	Payment of claims for care in the community	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Health Insurance Beneficiary Numbers/Account	MOU	Via secure file transfer protocol within the VA network, paper,	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)
		Numbers, Current Medications, Provider's TIN and Address information.		and/or by phone.	
Department of Defense (DOD)	Financial / Medical Information	Name (full), Social Security Number (Full), Date of Birth (Full) Mother's Maiden Name, Mailing Address, Zip Code Health Insurance Beneficiary Numbers, Account Numbers, Internet Protocol (IP) Address Numbers, Previous Medical Records, and Veteran Service-Connected Status and Conditions	23VA10NB3, 54VA10NB3, MOU, Computer Matching Agreement	Via secure file transfer protocol within the VA network, paper, and/or by phone.	VHA-IVC
Contractor system Emdeon (Change HealthCare) Corporate Data	Health Care clearing house services, data storage	Claims Status and Payment Information, Name (full), Social Security Number (Full), Date of Birth (Full) Mother's Maiden Name, Mailing Address, Zip Code Health Insurance Beneficiary Numbers, Account Numbers, Internet Protocol (IP) Address Numbers, Previous Medical Records, and Veteran Service-Connected Status and Conditions	Contract, ISA/MOU	Secure FTPS FIPS 140-2 Secure Transmission	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)*
Office of the Inspector General (OIG) - Office of the Inspector General (OIG) Legal Demand	Fraud, waste, & abuse	Name (full), Social Security Number (Full), Date of Birth (Full) Mother's Maiden Name, Mailing Address, Zip Code Health Insurance Beneficiary Numbers, Account Numbers, Internet Protocol (IP) Address Numbers, Previous Medical Records, and Veteran Service-Connected Status and Conditions	Legal Demand, MOU	Secure FTPS FIPS 140-2 Secure Transmission or UPS, or Fax	VHA-IVC
Office of Finance - Office of Finance - Improper Payments Elimination and Recovery Improvement Act (IPERIA)	Recovery Audit contract to recoup over payments and under payments made to the VA	Name (full), Social Security Number (Full), Date of Birth (Full) Mother's Maiden Name, Mailing Address, Zip Code Health Insurance Beneficiary Numbers, Account Numbers, Internet Protocol (IP) Address Numbers, Previous Medical Records, and Veteran Service-Connected Status and Conditions	MOU	Secure FTPS FIPS 140-2 Secure Transmission or UPS, or Fax	VHA-IVC
Optum RX (Pharmacy Clearinghouse)	Process, meds by mail and payment for prescriptions	Name, Social Security Number (SSN), Date of Birth (DOB), Address, Zip Code Health Insurance Numbers, CPY and International Code Designator (ICD)	Contract	Electronically pulled and pushed. Secure FTPS FIPS 140-2 Secure Transmission	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)*
		Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address		VIA VA network	
State Veteran's Home	Social Work Assessment	Name, Social Security Number (SSN), Date of birth (DOB), Address, Gender, age, physical (Health) information, Social Work Assessment, Medications, Service Connection Rating	Contract	SSL or create a VPN/IPSEC Tunnel as required by the State Homes Network security with the VA administrators to be installed on Linux servers	VHA-IVC
Adobe Experience Manager (AEM) Forms Managed Services - Enterprise	Social Work Assessment	Name, Social Security Number (SSN), Date of birth (DOB), Address, Gender, age, Physical information, Health Data, Social Work Assessment, Medications	Contract and Business Associate Agreement	SSL or create a VPN/IPSEC Tunnel as required by the State Homes Network security with the VA administrators to be installed	VHA-IVC

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 Boundary (VBA, VHA, NCA, Program Office)*
				on Linux servers	
Conduent Federal Solutions system - Conduent, system Burgess Reimbursement System (BRS)	Claims pricing services	Social Security Number, Zip Code, Veteran's diagnosis code, Procedure Codes), and Individually Identifiable Information (III).	Contract, National Business Associate Agreement, ISA/MOU	Web portal	VHA-IVC
HMS Federal - In-Sync (subcontractor to HMS Federal)	Recovery Audit contract to recoup over payments and under payments made to the VA	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI)	Business Associate Agreement (BAA)	Subcontractor enters contractor environment	VHA-IVC
Denver Regional Health District	Medical Records	Name, Date of Birth, Sex, SSN, demographics, health information	Title 38, United States Code, Section 5701; VHA Standing Letter agreement; SORN 79VA19	VIA Fax	VHA-ECHCS
Department of Public Health and Environment (DDPHE)	Medical Records	Name, Date of Birth, Sex, SSN, demographics, health information	VHA Standing Letter Agreement	Via secure web portal	VHA-ECHCS
Colorado State Department of Health; Death Certificates Office: via Electronic Death	Medical Records	Name, Date of Birth, Sex, SSN, demographics, health information	Local Agreement with Decedent Affairs	Via secure web portal	VHA-ECHCS

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 Boundary (VBA, VHA, NCA, Program Office)*
Registration System (EDRS)					
University of Colorado, Denver (UCHealth, Denver)	The purpose of this interconnection between the Department of Veterans Affairs (VA) Eastern Colorado Health Care System (ECHCS) and the University of Colorado Health (UCHealth) is to provide ECHCS's AGFA Picture Archival Communication System (PACS) a bidirectional two-way path through a site-to-site Virtual Private Network (VPN) tunnel to UCHealth PACS.	Name, Date of Birth, Sex, SSN, demographics, health information	Local MOU/ISA	Business Partner Gateway – VA TIC Gateway via a S2S VPN tunnel connection. Protected through the use of FIPS 140-2	VHA-ECHCS
Minuteman Technology Services	The purpose of the connection is to establish a bi-directional	First Name, Last Name, Middle Name, Veteran ID (or other unique identifier), Indicator for	Local MOU/ISA	Via Secure File Transfer Protocol (SFTP), using	VIA-ECHCS

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 Boundary (VBA, VHA, NCA, Program Office)
	site-to-site VPN 1) to transfer Veterans data from VA's system to NORC's system for the purpose of survey data collection and, 2) to transfer collected survey data from NORC's system back to VA's system.	whether person was living at the end of FY 2017 (or most recent FY available), Full Address, State name, County name of residence, Urbanicity (urban/rural),Urbanicity (urban/large rural/small rural/isolated), Telephone Number, Email Address, Date of Birth, Gender, Ethnicity, Race, Transition Status, Maximum separation date, Veteran Status, VHA usage information, Years of service, Retirement Indicator, Branch, Rank, Wars served in, Character of Service, Components served in, Branch of most recent separation, Benefits used, Benefits used 2 years prior to most recent year available, Benefits used 1 year prior to most recent year available, Active health insurance, An index of whether or not the Veteran is deemed competent enough to receive his/her		port 22, and using FIPS approved, 256-bit encryption	

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 Boundary (VBA, VHA, NCA, Program Office)*
		payments directly or whether they must be paid to a fiduciary, Unemployment status, Household income			
BOSS and Veterans Benefits Management Service (VBMS) – State and Tribal Cemeteries	Benefits, decedent, claimant, requestor, and beneficiary information	Names, addresses, service information, marriage/dependent status, and social security numbers.	MOU – in draft	Electronic access within the system	NCA – State and Tribal cemeteries located within the area.
Salesforce	The MBMS application will need to push/pull data from existing data sources via Rest APIs exposed by MBMS Functionality build includes Case Management Eligibility, and Scheduling	Names, addresses service information marriage/dependent status and social security numbers	48V40B – Veterans (Deceased) Headstone or Marker Records-VA per Title 38, United States Code, Sections 501(a), 501(b), and Chapter 24, Sections 2400-2404, ISA/MOU between Salesforce and MBMS System	Service Based	NCA State and Tribal cemeteries located within the area
VAEC AWS	AWS hosted VAEC is the government cloud that will serve as the infrastructure that hosts the	Names, addresses, service information, marriage/dependent status, and social security numbers.	MBMS is a minor application under the BIP Platform ATO – all VAEC AWS	Hosted Environment	NCA – State and Tribal cemeteries located within the area

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 Boundary (VBA, VHA, NCA, Program Office)
	BIP platform as a service and subsequent hosted minor application, MBMS		agreements are between BIP and VAEC		

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 disclosur e

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

Privacy Risk: The sharing of data is necessary for individuals to receive benefits at the *Area Denver*. 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 Boundary that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

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

The *Area Denver* 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 at https://www.oprm.va.gov/privacy/systems_of_records.aspx.

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	Applicable SORs
VHA	- Applicants for Employment Under Title 38, USC – VA, 02VA135, (Published Prior to 1995) - Automated Safety Incident Surveillance and Tracking System – VA, 99VA13, 3/31/2009 - Community Care (CC) Provider Profile Management System (PPMS) – VA, 1/25/2021Community Placement Program – VA, 186VA10D, 65VA122, 7/9/2009 - Community Residential Care and Medical Foster Home Programs – VA, 142VA114, 11/1/2011 - Compliance Records, Response, and Resolution of Reports of Persons Allegedly Involved in Compliance Violations – VA, 106VA17, 8/17/2009 - Customer Relationship Management System (CRMS) – VA, 155VA10NB, 3/3/2015 - Employee Medical File System Records (Title 38) – VA, 08VA05, 1/25/2023 - Enrollment and Eligibility Records – VA, 147VA10, 8/17/2021 - Health Care Provider Credentialing and Privileging Records – VA, 77VA10A4, 2/7/2020 - HealthShare Referral Manager (HSRM) – VA, 180VA10D, 8/17/2021 - Income Verification Records – VA, 89VA10, 3/23/2023 - Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attendings, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records – VA, 14VA135, 11/18/2010 - National Patient Databases – VA, 121VA10A7, 2/12/2018 - Non-VA Care (Fee) Records – VA, 23VA10NB3, 7/30/2015 - Patient Advocate Tracking System Replacement (PATS–R) – VA, 100VA10H, 1/25/2021 - Patient Medical Records – VA, 24VA10A7, 10/2/2020 - Police and Security Records – VA, 103VA07B, 10/21/2022 - Telephone Service for Clinical Care Records – VA, 113VA112, 5/8/2009 - The Revenue Program-Billing and Collections Records – VA, 114VA10, 1/25/2021 - Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA, 54VA10NB3, 3/3/2015 - Veterans, Dependents of Veterans, and VA Beneficiary Survey Records – VA, 43VA008, 1/25/2021

Site Type: VBA/VHA/NCA or Program Office	Applicable SORs
	• Veteran, Patient, Employee, and Volunteer Research and Development Project Records – VA, 32VA10Q, 6/23/2021 • Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, 79VA10, 12/23/2020 • VHA Corporate Data Warehouse – VA, 172VA10, 12/22/2021
VBA	• Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA, 58VA21/22/28, 11/8/2021
NCA	• Veterans and Dependents National Cemetery Gravesite Reservation Records -VA SOR 41VA41 • Veterans and Dependents National Cemetery Interment Records-VA SOR 42VA41 • Veterans (Deceased) Headstone or Marker Records-VA, SOR 48VA40B • VA National Cemetery Pre-Need Eligibility Determination Records -VA SOR 175VA41A

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

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

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

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

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

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

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

*[Review the suggested answer below and list any other information pertaining to the opportunity and right to decline to provide information. **Please remember processes at this boundary may differ from the standardized answer below].***

The *Area Denver* 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 Denver*.

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

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

Privacy Risk: There is a risk that veterans and other members of the public will not know that the *Area Denver* 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 Boundary are exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

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

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 myHealtheVet program, VA's online personal health record. More information about myHealtheVet program is available at https://www.myhealth.va.gov/mhv-portal-web/home.

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 at https://benefits.va.gov/benefits/offices.asp.

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.
<u>*Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.*</u>

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

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

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>
Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this Boundary and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to

be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

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

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

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

Privacy Risk: 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 Denver* 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.

VBA Mitigation: This privacy risk is mitigated by information provided in VA SOR Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA SOR 58VA21/22/28 (July 19, 2012). This states that individuals should contact their local VA regional office for additional information about accessing and contesting their records at the VA.

The *Area Denver* 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 Boundary, and are they documented?

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

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

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

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

Individuals receive access to the *Area Denver* by gainful employment in the VA or upon being awarded a contract that requires access to the boundary 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 Denver* 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 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 Denver* 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 Denver* 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 notify Divisions, IT and ISSO of new hires and their start date(s), either through email, fax, or a New Employee Orientation. 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 Boundary and the PII? If yes, what involvement will contractors have with the design and maintenance of the Boundary? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the Boundary?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the Boundary and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Contractors will have access to the 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 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 Denver* 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 Boundary?

VA offers privacy and security training. Each program or Boundary may offer training specific to the program or Boundary that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.

This question is related to privacy control AR-5, Privacy Awareness and Training.

All **Area Denver** 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 Boundary 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 Boundary?

8.4a If Yes, provide:

1. *The Systems Security Plan Status: Approved*
2. *The Systems Security Plan Status Date: June 29, 2021*
3. *The Authorization Status: Authorization to Operate (ATO)*
4. *The Authorization Date: September 8, 2021*
5. *The Authorization Termination Date: September 7, 2024*
6. *The Risk Review Completion Date: August 4, 2021*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): Moderate*

Please note that all Boundaries 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 Boundary Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	Boundary of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

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

Signature of Privacy Officers

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

Privacy Officer, Eller Pamintuan

Privacy Officer, Dana Krishland

Privacy Officer, Daniel Quigley

Privacy Officer, Cindy Merritt

Signature of Information System Security Officers

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

Information System Security Officer, Ashton Botts

Information System Security Officer, Je'Nean Clark

Information System Security Officer, Eduardo Lorenzo

Information System Security Officer, Bernadette Bowen-Welch

Signature of Area Manager

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

Area Manager, Jim Hughes

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 Mapping of Components (Servers/ Database))

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
• Server: 1 Cardio perfect	Yes	Yes	Yes	Social Security Number, EKG reading, Blood Pressure	Consolidated SQL database for multiple applications	Logical Access to Servers is limited to SQL team. Physical Access is limited. Server is Encrypted.	VBA
• Server: 2 • VBMS	Yes	Yes	Yes	Disability/Compensation	Consolidated SQL database for multiple applications	Logical Access to Servers is limited to SQL team. Physical	VBA

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
						Access is limited. Server is Encrypted.	
• Server: 3 • NOPSWorkstationV2 • VCS Dashboard	Yes	Yes	Yes	Name, Social Security Number (SSN), Member Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and	Consolidated SQL database for multiple applications	Logical Access to Servers is limited to SQL team. Physical Access is limited. Server is Encrypted.	VHA-ECHCS

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				International Code Designator (ICD), Coded Billing Information, Health Information, Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate			

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				Veteran with Beneficiary.			
• Server: 4 • dbNetepay	Yes	Yes	Yes	Name, Social Security Number (SSN), Member Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and International Code Designator	Consolidated SQL database for multiple applications	Logical Access to Servers is limited to SQL team. Physical Access is limited. Server is Encrypted.	VHA-ECHCS

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				(ICD), Coded Billing Information, Health Information, Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
• Server: 5 • Censis_Beta_V2_Global • censis_graphics • Censis_HL1301	Yes	Yes	Yes	Name, Social Security Number (SSN), Member	Consolidated SQL database for multiple applications, EndoVault,	Logical Access to Servers is limited to SQL team. Physical Access is limited. Server is Encrypted.	VHA-ECHCS

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
• Censis_SG1301 • CensisBufferAgent • CLOPID_SCRIPTS • CLOPIDOGREL • ClopidTemp • ECHDynaTouch • EFORMS • EMR • EncoreDB • EncoreWarehouse • Hibernate • HYP • IntelliWare • IVR • IVRAccess • jacrabbit • LICENSE • Maintenance • ManitenanceLog • Medication_Adherence • mipacs_db • MiPACS_viewer_db • MRSLIVE				Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and International Code Designator (ICD), Coded Billing Information, Health Information, Prescription Information, Procedure	PACS, MGC Diagnostics, Respironics		

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
• Prophecy • PROST • qp_agent • qp_app • qp_auditing • qp_calendar • qp_central • quartzqm • ReportServer • ReportServerTempDB • Research_IVR_DB • SentryConnectGateway • SentrySuite • SentryWorklist • SEPPRMACI • SOLUTIONINFO • Statdb • VcmEchLive • VcmEchTest • VHAECH HR ERLR • VHAECH HR FEE BASIS • VHAECH HR PERFORMANCE				Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
• VHAECH HR STAFFING • VHAECH HR WOC • WEBAPPCONFIG • WICMASTER							
• Server: 6 • Cochlear_Database • NOAHDatabaseCore	Yes	Yes	Yes	Name, Social Security Number (SSN), Member Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and	Consolidated SQL database for multiple applications, NOAH, Intelliwave, Romexis	Logical Access to Servers is limited to SQL team. Physical Access is limited. Server is Encrypted	VHA-ECHCS

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				International Code Designator (ICD), Coded Billing Information, Health Information, Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
• Server: 7 • CART_RTLS_1	Yes	Yes	Yes	Name, Social Security	Consolidated SQL database for	Logical Access to Servers is limited to	VHA-ECHCS

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
• CART_RTLS_2 • CART_V4_AutoTest_1 • CartLogArchive • CARTModel_V4 • CartPro4 • FDA • IVR • MAE • SSISDB				Number (SSN), Member Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and International Code Designator (ICD), Coded Billing Information, Health Information,	multiple applications	SQL team. Physical Access is limited. Server is Encrypted.	

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
• Server: 8 • CLOPID_SCRIPTS • CLOPIDOGREL • ClopidTemp • HYP • IVR • IVRAccess • Medication_Adherence	Yes	Yes	Yes	Name, Social Security Number (SSN), Member Identification Number, Patient Control Number, Medical	Consolidated SQL database for multiple applications, NOAH, Intelliwave, Romexis	Logical Access to Servers is limited to SQL team. Physical Access is limited. Server is Encrypted	VHA-ECHCS

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
• Prophecy • PROST • ReportServer • ReportServerTempDB • Research_IVR_DB • SEPPRMACI				Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and International Code Designator (ICD), Coded Billing Information, Health Information, Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification			

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
• Server: 9 • ExtraView19 • iMed37 • iMedAudit • SentrySuite • SentrySuiteTest • UpdateHistory	Yes	Yes	Yes	Name, Social Security Number (SSN), Member Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if	Consolidated SQL database for multiple applications Such as Imed consent	Logical Access to Servers is limited to SQL team. Physical Access is limited. Server is Encrypted	VHA-ECHCS

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				appropriate), Health Insurance Numbers, and International Code Designator (ICD), Coded Billing Information, Health Information, Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate			

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				Veteran with Beneficiary.			
• Server: 10 • PluTtlDC • PluTtlDS • PluTtlPC • PluTtlPS • PluTtlTC	Yes	Yes	Yes	Name, Social Security Number (SSN), Member Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and International Code Designator (ICD), Coded	Consolidated SQL database for multiple applications	Logical Access to Servers is limited to SQL team. Physical Access is limited. Server is Encrypted.	VHA-ECHCS

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				Billing Information, Health Information, Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
• Server: 11 • ActiveSurvey • CART_EP • CART_RTLS_1 • CART_V4_AutoTest_1	Yes	Yes	Yes	Name, Social Security Number (SSN), Member Identification	Consolidated SQL database for multiple applications	Logical Access to Servers is limited to SQL team. Physical Access is limited. Server is Encrypted.	VHA-ECHCS

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
• CART_V4_Dev • CART2CDWCART • CARTModel_V4 • CARTPro4 • CARTWebDev1 • CARTWebMAE • CARTWebRPDev1 • CARTWebSiteReviews • FastADABoost • FDA • IVR • MAE • ReportServer • ReportServerTempDB • SSISDB				Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and International Code Designator (ICD), Coded Billing Information, Health Information, Prescription Information, Procedure Codes			

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
• Server: 12 • PluTtlDC • PluTtlDS • PluTtlPC • PluTtlPS • PluTtlTC	Yes	Yes	Yes	Name, Social Security Number (SSN), Member Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth	Consolidated SQL database for multiple applications	Logical Access to Servers is limited to SQL team. Physical Access is limited. Server is Encrypted.	VHA-ECHCS

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				(DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and International Code Designator (ICD), Coded Billing Information, Health Information, Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health			

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				Insurance Beneficiary Information to associate Veteran with Beneficiary.			
• Server: 13 • CoreyMapping • crystal • IPA_R54_VA_DENVER • mirthdb • PAREXBASE_ECH • SFFX • SFFXResearch	Yes	Yes	Yes	Name, Social Security Number (SSN), Member Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and	Consolidated SQL database for multiple applications	Logical Access to Servers is limited to SQL team. Physical Access is limited. Server is Encrypted.	VHA-ECHCS

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				International Code Designator (ICD), Coded Billing Information, Health Information, Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
• Server: 14 • AppStudioDB	Yes	Yes	Yes	Name, Social Security	Consolidated SQL database for	Logical Access to Servers is limited to	VHA-ECHCS

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
• AuditDB • CacheDB • CommServ • CVCloud • DM2 • HistoryDB • ResourceMgrDB • TemplateDB • WFEngine				Number (SSN), Member Identification Number, Patient Control Number, Medical Record Identification Number, Date of Birth (DOB), Address; Zip Code, Email, Fax (if appropriate), Health Insurance Numbers, and International Code Designator (ICD), Coded Billing Information, Health Information,	multiple applications	SQL team. Physical Access is limited. Server is Encrypted.	

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
• Server: 15 • State Home Per Diem Program (SHPDP) Office	Yes	Yes	Yes	Name, SSN, Date of birth (DOB), Address, Gender, Age, Physical information, Health Data, Social Work	The data is utilized to positively identify the Veteran and/or beneficiary.	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA-IVC

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				Assessment, Medications			
• Server: 16 • State Home Per Diem (SHPD) Web Application	Yes	Yes	Yes	Name, SSN, Address, Medical Condition, Health Data, Service Connection Rating	The data is utilized to positively identify the Veteran and/or beneficiary.	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA-IVC
• Server: 17 • Adobe Experience Manager (AEM)	Yes	Yes	Yes	Name, SSN, Address, Medical Condition, Health Data, Service Connection Rating	The data is utilized to positively identify the Veteran and/or beneficiary.	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA-IVC
• Server: 18 • HMS SharePoint	Yes	Yes	Yes	name, date of birth (DOB), Social Security Number (SSN), address, diagnosis codes, procedure codes, date of	Used for determining eligibility and processing veteran/beneficiary claims.	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA-IVC

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				service, type of service, place of service, claim amounts			
• Servers: 19 • HealthcareAppeals (Cyrstal Reports)	Yes	Yes	Yes	Social Security Number; Beneficiary Name	The data is utilized to positively identify the Veteran and/or beneficiary.	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA-IVC
• Servers: 20 • Right Fax	Yes	Yes	Yes	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number, Fax Number, Email Address	Used for transmitting/exchanging EOBs and veteran/beneficiary claims information between VHA and healthcare providers.	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA-IVC
• Servers: 21	Yes	Yes	Yes	Name, social security number, date of birth, mailing	Used for determining eligibility and processing	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and	VHA-IVC

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
• CLAIMS_ATTACHMENTS (Payer Operating Rules (POR) Attachments)				address, zip code, phone numbers, current medications, Previous Medical Records/biometrics, Provider name, provider address, provider telephone number, National Provider Identifier (NPI), financial information	veteran/beneficiary claims.	managed with restricted access controls	
• Servers: 22 • Eligibility • Mental Health Certification Program (MHCP)	Yes	Yes	Yes	Veteran/Beneficiary: Name, Social Security Number, telephone number, member	Used for determining eligibility and processing veteran/beneficiary claims.	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA-IVC

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				Identification Number, address, email, health information, financial information, biometrics. Provider: Name, Business name, Address, Telephone, National Provider Identifier (NPI), financial information			
• Servers: 23 • Appeals Management Tool (IMGRPTS)	Yes	Yes	Yes	Veteran/Beneficiary: Name, Social Security Number, telephone number, member	Used for determining eligibility and processing veteran/beneficiary claims, specifically for	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA-IVC

Components of the 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	Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)
				Identification Number, address, email, health information, financial information, biometrics. Provider: Name, Business name, Address, Telephone, National Provider Identifier (NPI), financial information	claims that have been appealed.		

APPENDIX C – List of Medical Devices and Special Purpose Systems

This table is only to be completed for the Medical Devices or Special Purpose System Boundary PIAs. This table should be skipped for the Area Boundary PIA. This information must match the medical devices and special purpose systems listed in 3.7 of the Boundary PTA.

Name of Device	Type (Medical Device or Special Purpose System)	Is the device within the MedMOD boundary?	Enterprise Risk Assessment Number