Date PIA submitted for review:
6/4/2021

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

Area Denver

Continental District

Facilities Supported by the Area:

1. Rocky Mountain Regional VA Medical Center	2. VA Health Administration Center (HAC)
3. Denver Regional Benefit Office (VBA)	4. 4A RCS Western Mountain Regional Office
5. Alamosa/San Luis Valley Clinic/ Sierra Blanca Medical Center	6. Aurora Community Based Outpatient Clinic (CBOC)
7. Bioscience	8. Boulder Vet Center
9. Colorado Springs PFC Floyd K Lindstrom CBOC	10. Burlington VA Outreach Clinic
11. Pavilion Towers (OIG)	12. Colorado Springs Vet Center
13. U. S. Air Force Academy (USAFA) 10th Medical Group	14. Continental VBA District Office

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

15. Continental Regional Counsel District Office	16. C&P VBA Training Facility
17. Denver A Interim Data Center	18. Denver B Interim Data Center
19. Denver Combat Call Center	20. Denver Homeless Domiciliary
21. Continental Memorial Service Network	22. Denver VA Community Resource and Referral Center (CRRC)
23. Denver Vet Center	24. Fisher House
25. Golden CBOC	26. IDES Fort Carson
27. IDES USAFA	28. Intake Site at Buckley Air Force Base (AFB)
29. Intake Site at Fort Carson	30. Intake Site at Peterson AFB
31. Intake Site at Schriever AFB	32. Intake Site at USAFA
33. Jewell CBOC	34. La Junta CBOC
35. Lamar CBOC	36. Pueblo NHCU (CLC)
37. Pueblo CBOC	38. Pueblo Vet Center
39. Rose CBOC	40. Salida VA Telehealth Clinic
41. SAO West, NCO 19 Rocky Mtn. Acquisition Center	42. Denver VA Domiciliary
43. VBA Human Resource Center Denver	44. VISN 19: Rocky Mountain Network
45. Vocational Rehabilitation Office - Colorado Springs	46. Western Public Affairs Office
47. Colorado Springs Union CBOC	50.

Area Boundary Contacts:

Area Privacy Officer

Name	Phone Number	Email Address	Location
Robert McGinn	719-227-4043	Robert.McGinn@va.gov	ECHCS
Dana Krishland	720-723-6765	Dana.Krishland@va.gov	ECHCS
Julie Drake	303-331-7823	Julie.Drake@va.gov	HAC
Daniel Quigley	303-914-5875	Daniel.Quigley@va.gov	VBA

Area Information System Security Officer

Name	Phone Number	Email Address	Location
Nichelle R. Downing	720-857-5273	Nichelle.Downing@va.gov	VHA
Ashton Botts	303-398-7155	Ashton.Botts@va.gov	HAC
Eduardo Lorenzo	303-914-5889	Eduardo.Lorenzo@va.gov	VBA
DeEtta Chagnon	(303) 325-6178	DeEtta.Chagnon@va.gov	VHA

Area Manager

Name	Phone Number	Email Address	Location
Jim Hughes	303-331-7898	Jim.Hughes@va.gov	ECHCS/HAC/VBA

Legend:

RED Text = Provides instructions and guidance for completing referenced sections or requires modification to be applicable to the area.

Blue Text (**VHA**) = Sample responses and language for **VHA** to be modified by the team completing the PIA.

Purple Text (**VBA**) = Sample responses and language for **VBA** to be modified by the team completing the PIA

Green Text (**HAC**) = Sample responses and language for **HAC** to be modified by the team completing the PIA

***All red instructional text as well as text not applicable to the Area must be removed. Text must be black before PIA is submitted to PIA Support.**

Abstract

Area Denver is an Information Area Boundary that consists of Rocky Mountain Regional Medical Center, VA Health Administration Center Denver, Denver Regional Benefit Office, 4A RCS Western Mountain Regional Office, Alamosa /San Luis Valley Clinic/Sierra Blanca Med. Ctr., Aurora Outpatient Clinic, Bioscience, Boulder Vet Center, Burlington VA Outreach Clinic, Pavilion Towers (OIG), Colorado Springs Clinic PFC Floyd K Lindstrom Clinic, Colorado Springs Vet Center, Colorado Springs 10th Medical Group Building, Continental VBA District Office, Continental Regional Counsel District Office, C&P VBA Training Facility, Denver A Interim Data Center, Denver B Interim Data Center, Denver Combat Call Center, Denver Homeless Domiciliary, Continental Memorial Service Network, Denver VA Community Resource and Referral Center, Denver Vet Center, Fisher House, Fort Logan National

Cemetery, Fort Lyon National Cemetery, Pikes Peak National Cemetery, Golden Outpatient Clinic, IDES Fort Carson, IDES US AFB Academy, Intake Site at Buckley Air Force Base, Intake Site at Fort Carson, Intake Site at Peterson Air Force Base, Intake Site at Schriever Air Force Base, Intake Site at USAF Academy, Jewell Clinic, La Junta Outpatient Clinic, Lamar Outpatient Clinic, Pueblo NHCU, Pueblo Outpatient Clinic, Pueblo Vet Center, Rose CBOC, Salida VA Telehealth Clinic, SAO West, NCO 19 Rocky Mtn. Acquisition Center, Denver VA Domiciliary, VBA Human Resource Center Denver, VISN 19: Rocky Mountain Network, Vocational Rehabilitation Office - Colorado Springs, Western Public Affairs Office. The Area Boundary environment consists of components such as workstations, laptops, portable computing devices, terminals, servers, printers, and IT enabled networked medical devices that are owned, managed, and maintained by the facilities. The Area provides operational connectivity services necessary to enable users' access to information technology resources throughout the enterprise including those within the facility, between facilities, resources hosted at data centers, and connectivity to other systems. Network connectivity rules are enforced by VA approved baselines for router and switch configurations. The Area Boundary system environment also includes as applicable, subsystem storage utilities such as tape drives, optical drives, disk drives, network area storage (NAS), storage access networks (SAN), archival appliances, special purpose systems, and tier 2 storage solutions. The Area Boundary encompasses the management, operational, and technical security controls associated with IT hardware, consisting of servers, routers, switches, hubs, gateways, peripheral devices, desktop/laptops, and OS software. The Area Boundary employs a myriad of routers and switches that connect to the VA network.

Overview

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

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

- *NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?*
- *What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the Cloud Service Provider or its customers (VA) be affected?*

Area Denver itself does not collect, use, disseminate, maintain, or store PII/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 Area will be referenced in this document since the Area IT boundary does not maintain, disseminate or store information accessed by each facility. PII/PHI.

The facilities within the Area IT Boundary collect, use, and/or disseminate PII/PHI that is maintained and stored within enterprise systems such as VistA, VBMS, BOSS/AMASS, etc. There are individual PIAs located here (https://www.oprm.va.gov/privacy/pia.aspx) that contain detailed information on the maintenance, dissemination and sharing practices, and storage of the PII/PHI for each Enterprise system accessed by the facilities.

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 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).

HAC - Denver HAC (DEN-HAC) 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 Denver HAC (DEN-HAC) 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.

Denver HAC (DEN-HAC) 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 Denver HAC (DEN-HAC) 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. The Area contains and transmits Personal information, health information, military benefits and disability rating, and financial information on veterans, their dependents, employees, and contractors. There are an estimated 1,418,429 individuals have their information stored at the Denver HAC (DEN-HAC) Site.

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. Denver HAC (DEN-HAC) 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.

Denver HAC (DEN-HAC) 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 HAC 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.

The applicable SORs for Area Denver include:

Applicable SORs

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	***Applicable SORs***
VHA (ECH)	• Non-VA Fee Basis Records-VA, SOR 23VA10NB3 • Patient Medical Records-VA, SOR 24VA10P2 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA12 • Community Placement Program-VA, SOR 65VA122 • Health Care Provider Credentialing and Privileging Records-VA,SOR 77VA10E2E • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10P2 • Income Verification Records-VA, SOR 89VA10NB • Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA13 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10D

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	*Applicable SORs*
	• National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147VA10NF1 • VHA Corporate Data Warehouse- VA 172VA10P2 • Applicants for Employment under Title 38, USC-VA, SORN 02VA135 • Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attendings, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records-VA, SORN 14VA05 (Nov. 18, 2010) • Patient Medical Records-VA, SORN 24VA19 (Nov 19, 2009) • Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA, SORN 34VA12 (May 27, 2010) • Community Placement Program-VA, SORN 65VA122 • Health Care provider credentialing and Privileging Records-VA,SORN 77VA10Q (March 26, 2008) • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SORN 79VA10P2 (Oct. 31, 2012, as amended) • Income Verification Records-VA, SORN 89VA19 (May 8, 2008) • Automated Safety Incident Surveillance and Tracking System-VA, SORN 99VA13 (March 31, 2009) • Telephone Service for Clinical Care Records- VA, SORN 113VA112 (May 8, 2009) • The Revenue Program Billings and Collection Records-VA, SORN 114VA16 (Dec. 10, 2009, as amended) • National Patient Databases-VA, SORN 121VA19 (May 11, 2012, as amended) • Patient Advocate tracking System (PATS)-VA, SORN 100VA10NS10 • Compliance Records, Response, and Resolution of reports of Persons Allegedly Involved in Compliance Violations-VA, SORN 106VA17 • Community Residential Care and Medical Foster Home Program-VA, SORN 142VA114 • Employee Medical Files System Records-VA, SORN Title 5: OPM/GOVT-10 • Employee Medical File System Records (Title 38)-VA, SORN 08VAO5 • Police and Security Records-VA, SORN 103VAO7B • 54VA10NB3, ‘‘Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files-VA’’ (March 3. 2015) • 55VA10NB, Customer Relationship Management System (CRMS) • 43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records-VA
VBA	• Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	*Applicable SORs*
HAC	• Patient Medical Records-VA, SOR 24VA10P2 • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10P2 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10D • National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147VA10NF1 • VHA Corporate Data Warehouse- VA 172VA10P2 • 54VA10NB3, ''Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files-VA'' (March 3. 2015) • 55VA10NB, Customer Relationship Management System (CRMS) 23VA10NB3, "Non-VA Care (Fee) Records-VA (FR: Thursday, July 30, 2015) 180VA10D, "HealthShare Referral Manager (HSRM)-VA" 186VA10D``Community Care (CC) Provider Profile Management System (PPMS)-VA"

Section 1. Characterization of the Information

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

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

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

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

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

☒ Name

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

- Age
- Biometrics
- Certificate/License numbers
- Contractor Mailing Address
- Contractor Name
- Contractor Personal Telephone Number
- Criminal background information
- Current Medications
- Date of Birth
- Date of Service
- Death certificate information
- Demographics
- Dental Eligibility
- Disclosure requestor information
- Education Information
- Electronic Protected Health Information (ePHI)
- Eligibility Date
- Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Employment information
- Fax Number
- Financial Account Information
- Gender
- Guardian Information
- Health Insurance Beneficiary Account Numbers
- Internal control Number
- International Code Designator (ICD), diagnosis codes
- Internet Protocol (IP) Address Numbers

- Mailing Address
- Medical Record Number
- Member ID
- Military history/service connection
- Mother's Maiden Name
- Name
- Next of Kin
- Other Health Insurance (OHI)
- Phone Number(s)
- Place of Service
- Previous Medical Records
- Procedure Codes/Coded Billing
- Race/Ethnicity
- Referral
- Rendering Provider Zip Code
- Service-connected disabilities
- Social Security Number
- Social Work Assessment/Electronic Protected Health Information (ePHI)
- Tax Identification Number (TIN)
- Tumor PII/PHI statistics
- VA Employee Name
- VA Login Identification (ID)
- Vehicle License Plate Number
- Veteran dependent information
- Zip Code

VBA – Other personal information accessible through the GSS include bank account information, employment history, gross income, and net worth information. The record, or information contained in the record, may include identifying information (e.g., name, address, social security number); military service and active duty separation information (e.g., name, service number, date of birth, rank, sex, total amount of active service, branch of service, character of service, pay grade, assigned separation reason, service period, whether veteran was discharged with a disability, reenlisted, received a Purple Heart or other military decoration); payment information (e.g., veteran payee name, address, dollar amount of readjustment service pay, amount of disability or pension payments, number of non-pay days, any amount of indebtedness (accounts receivable) arising from title 38 U.S.C. benefits and which are owed to the VA); medical information (e.g., medical and dental treatment in the Armed Forces including type of service-connected disability, medical facilities, or medical or dental treatment by VA health care personnel or received from private hospitals and health care personnel relating to a claim for VA disability benefits or medical or dental treatment); personal information (e.g., marital status, name and address of dependents, occupation, amount of education of a veteran or a dependent, dependent's relationship to veteran); education benefit information (e.g., information arising from utilization of training benefits such as a veteran trainee's

induction, reentrance or dismissal from a program or progress and attendance in an education or training program); applications for compensation, pension, education and vocational rehabilitation benefits and training which may contain identifying information, military service and active duty separation information, payment information, medical and dental information, personal and education benefit information relating to a veteran or beneficiary's incarceration in a penal institution (e.g., name of incarcerated veteran or beneficiary, claims folder number, name and address of penal institution, date of commitment, type of offense, scheduled release date, veteran's date of birth, beneficiary relationship to veteran and whether veteran or beneficiary is in a work release or half-way house program, on parole or has been released from incarceration).

PII Mapping of Components

Area Denver consists of 31 total components 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 Area Boundary?

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

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

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

VBA – The below are All Nationwide databases/systems, NOT located at Denver RO, but used by the Denver RO employees.

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

Additional sources include:

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

1.3 How is the information collected?

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

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

ECH - Information collected directly from patients, employees and/or other members of the public is collected using paper forms (such as the enrollment form for VA health care), or interviews and assessments with the individual. Information from outside resources comes in several ways. For example, military records from the Department of Defense (DoD) are sent to VBA using encrypted electronic transmission for eligibility determination and processing.

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

VBA - There are many VA forms used by veterans to apply for and/or make adjustments to pending benefits. All VBA benefit forms are located at http://www.va.gov/vaforms/. The URL of the associated privacy statement is: http://www.va.gov/privacy/. VBA forms can be downloaded from this site, filled in and printed to be delivered in paper form. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury.

The VBA toll free number for veterans is 1-800-827-1000. Clients are referred to and transferred to the Regional Office of Jurisdiction, where they can provide a service representative with required information. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury. VBA employees may also contact a veteran directly to obtain clarifying information for a claim for benefits

Means of Collection Table

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	***Means of Collection***
VHA	Information collected directly from patients, employees and/or other members of the public is collected using paper forms (such as the VA Form 10-10EZ enrollment form for VA health care), or interviews and assessments with the individual. Much of the information provided by veterans or other members of the public, such as address and phone number, next of kin and emergency contact information, and similar information are assumed to be accurate because it is provided directly by the individual. Additionally, information entered into an individual's medical record by a doctor or other medical staff is also assumed to be accurate.
VBA	There are many VA forms used by Veterans to apply for and/or make adjustments to pending benefits. All VBA benefit forms are located at http://www.va.gov/vaforms/. The URL of the associated privacy statement is: http://www.va.gov/privacy/. VBA forms can be downloaded from this site, filled in and printed to be delivered in paper form. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury. The VBA toll free number for veterans is 1-800-827-1000. Clients are referred to and transferred to the Regional Office of Jurisdiction, where they can provide a service representative with

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	*Means of Collection*
	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.
HAC	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.

Information related to an employee's employment application may be gathered from the applicant for employment, which is provided to an application processing website, USA Jobs located at https://www.usajobs.gov/.

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.

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

Include a statement of why the particular PII/PHI is collected, maintained, used, or disseminated in the Area Boundary is necessary to the program's or agency's mission. Merely stating the general purpose of the Area Boundary without explaining why this particular type of information should be collected and stored is not an adequate response to this question.
If the Area Boundary collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the Area Boundary's purpose. This question is related to privacy control AP-2, Purpose Specification.

The purposes of the information from Veterans and other members of the public collected, maintained, and processed by 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.

ECH - The purposes of the information from veterans and other members of the public collected, maintained, and processed by the GSS systems are as varied as the types of information collected. The purposes include:
1. To determine eligibility for health care and continuity of care
2. Emergency contact information in cases of emergency situations such as medical emergencies
3. Provide medical care
4. Communication with veterans/patients and their families/emergency contacts
5. Determine legal authority for providers and health care workers to practice medicine and/or subject matter expertise
6. Responding to release of information requests
7. Third party health care plan billing, e.g. private insurance
8. Statistical analysis of patient treatment
9. Contact for employment eligibility/verification

In the case of employment and employee related records, the primary types of information collected, retained, and used is for:

• To determine eligibility for employment
• To withhold and report earnings to Federal, state, and local tax collection agencies
• To provide compensation and benefits to employees for services provided to the agency
• To provide Occupational Health services to employees who are injured or fall ill during their duty day

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

Much of the information collected is maintained, used, and disseminated to ensure that Veterans and other eligible individuals obtain the medical and mental health treatment they require. Additional information, such as bank account information and insurance information are used to process claims and requests for benefits. Other purposes include determination of legal authority for providers and other clinical staff to practice medicine and/or subject matter expertise, release of information request responses, and research/analysis of data.
1. To determine eligibility for health care and continuity of care
2. Emergency contact information is cases of emergency situations such as medical emergencies
3. Provide medical care
4. Communication with Veterans/patients and their families/emergency contacts
5. Determine legal authority for providers and health care workers to practice medicine and/or subject matter expertise
6. Responding to release of information request
7. Third party health care plan billing, e.g. private insurance
8. Statistical analysis of patient treatment
9. Contact for employment eligibility/verification

VBA - The VBA benefit systems accessed through the GSS, process entitlements for five mission areas: Compensation and Pension, Education, Vocational Rehabilitation and Employment, Loan

Guaranty, and 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. The information collected includes: Name, Address, Social Security Number, Family/Dependents, marital status, medical status, birth information, death information, service data; Reserve or Guard Participation, retired pay or severance pay, hazardous agent exposure, branch of service, duty date, released date, type of discharge, separation reason, medical records, military clinical records, government health records, vocational rehabilitation and employment records, line of duty investigations to include police reports; incarceration at federal, state or local facility, fugitive felon status, and/or investigative reports for some accidents. The records may also contain additional veteran information such: Guardian information; court proceedings, field examinations, appointment and bonding of fiduciaries, and annual accounts. The benefit systems accessed through the GSS also contain veteran educational records such as: education program approval information, approved courses, effective dates, types of training, facility code, objective code, and training type. Income verification is also used for veteran pension-based decisions and entitlements. Most of the information provided above is kept in a central database not located at this facility but any of this information could be stored on the GSS at any given time during or after the processing of a VBA benefit.

Purpose of Information Collection Table

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

HAC	• 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

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

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

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

Information 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.

ECH - 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. Additionally, the Veterans Benefit Administration provides verification that veterans and their dependents are eligible for the benefits they are claiming.

HAC - 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.

VBA - All data are matched against supporting claims documentation submitted by the veteran, widow, or dependent. Certain data such as SSN is verified with the Social Security Administration. Prior to any award or entitlement authorization(s) by the VBA, the veteran record is manually reviewed, and data validated to ensure correct entitlement has been approved.

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

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

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

ECH - The GSS maintained under the authority of Veterans' Benefits Act, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)
The collection and processing of health information must follow the rules and regulations established by the:
• Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).
• Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.

HAC –

- 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
- Title 38 United States Code 5701, 7332
- VHA Directive 1605.01 Privacy & Release of Information
- VA Directive 6500 Managing Information Security Risk: VA Information Security Program.
- 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.
- Public Law 103–446, section 107 and Public Law 111–163 section 101.
- Public Law 111–163 section 101

VBA - Generally, the authority to operate the Veterans 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 510, and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55. This information is reflected in the VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28 (July 19, 2012). 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 552a(a)(4).1.575(b); 38 CFR 14.631; 38 USC 5101(c); 38 U.S. Code 7703; Title 5 USC 552a(a)(4).

Legal Authority Table

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	Legal Authority
VHA	• Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a) • Health Insurance Portability and Accountability Act of 1996 (HIPAA) • Privacy Act of 1974 • Freedom of Information Act (FOIA) 5 USC 552 • VHA Directive 1605.01 Privacy & Release of Information • VA Directive 6500 Managing Information Security Risk: VA Information Security Program. • Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.
VBA	• Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b) • Authority to operate the Veterans 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 510, and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55. This information is reflected in the VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28 (July 19, 2012). 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 552a(a)(4).1.575(b); 38 CFR 14.631; 38 USC 5101(c); 38 U.S. Code 7703; Title 5 USC 552a(a)(4).
HAC	• 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

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	Legal Authority
	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. Public Law 103–446, section 107 and Public Law 111–163 section 101.Public Law 111–163 section 101

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

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

Privacy Risk:

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 area employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

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

Section 2. Uses of the Information

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

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

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

• Age: Used to run analytics regarding care provided
• Biometrics: Used for access controls, identification purposes
• Certificate/License numbers: Used to track and verify legal authority to practice medicine and licensure for health care workers in a particular area of expertise.
• Contractor Mailing Address: Used to determine VA employment eligibility and for veteran contact, financial verification.
• Contractor Name: Used to determine VA employment eligibility and for veteran contact, financial verification.
• Contractor Personal Telephone Number: Used to determine VA employment eligibility and for veteran contact, financial verification.
• Criminal background information: Used to determine employment eligibility and during VA Police investigations.
• Current Medications: Used within the medical records for health care purposes/treatment, prescribing medications, and allergy interactions.

• Date of Birth: Used to identify age and confirm patient identity
• Date of Service: Used to match authorization to claims submitted for payment
• Death certificate information: Used to determine date, location and cause of death.
• Demographics: Used to run analytics reports for leadership
• Dental Eligibility: Used for continuity of health care and payment
• Disclosure requestor information: Used to track and account for patient medical records released to requestors.
• 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
• Electronic Protected Health Information (ePHI): Used for history of health care treatment, during treatment and plan of treatment when necessary.
• Eligibility Date: Used to pay associated care
• Email Address: used for communication and my HealtheVet secure communications
• Emergency Contact Information (Name, Phone Number, etc. of a different individual): Used in cases of emergent situations such as medical emergencies.
• Employment information: Used to determine VA employment eligibility and for veteran contact, financial verification.
• Fax Number: used to send forms of communication and records to business contacts, insurance companies and health care providers
• Financial Account Information: Used to calculate co-payments and VA health care benefit eligibility
• Gender: Used as patient demographic, identity, and indicator for type of medical care/provider and medical tests required for individual.
• Guardian Information: Used when patient is unable to make decisions for themselves.
• Health Insurance Beneficiary Account Numbers: Used to communicate and bill third part health care plans
• Internal control Number: Used to track patient payment records
• International Code Designator (ICD), diagnosis codes: Used for payment internal and external to the VA
• Internet Protocol (IP) Address Numbers: Used for configuration and network connections. Network Communication, allowing information to be transferred from one Information Technology system to another.
• Mailing Address: Used for communication, billing purposes and calculate travel pay
• Medical Record Number: Used as a patient identifier to provide services to enrolled and eligible Veterans.
• Member ID: Used for care of veterans
• Military history/service connection: Used to evaluate medical conditions that could be related to location of military time served. Also used to determine VA benefit and health care eligibility.
• Mother's Maiden Name: Used to confirm patient identity
• Name: Used to identify the patient during appointments and in other forms of communication
• Next of Kin: Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
• Other Health Insurance (OHI): Used to bill for care as the first party payer
• Phone Number(s): Used for communication, confirmation of appointments and conduct telehealth appointments
• Place of Service: Used to verify authorizations
• Previous Medical Records: Used for continuity of health care
• Procedure Codes/Coded Billing: Used in the payment of claims

• Race/Ethnicity: Used for patient demographic information and for indicators of ethnicity- related diseases.
• Referral: Used in the payment of claims
• Rendering Provider Zip Code: Used for communication, billing purposes, and calculate travel pay
• Service-connected disabilities: Used to determine VA health care eligibility and treatment plans/programs
• Social Security Number: Used as a patient identifier and as a resource for verifying income information with the Social Security Administration
• Social Work Assessment/Electronic Protected Health Information (ePHI): Used for history of health care treatment, during treatment and plan of treatment when necessary.
• Tax Identification Number (TIN): Used to pay community providers
• Tumor PII/PHI statistics: Used to track and trend statistical data regarding cancerous diseases.
• VA Employee Name: Used to monitor access controls
• VA Login Identification (ID): Used to monitor access controls
• Vehicle License Plate Number: Used by VA Police in completing Uniformed Officer Reports (UOR) with incidents involving vehicles.
• Veteran dependent information: Used to determine benefit support and as an emergency contact person
• Zip Code: Used for communication, billing purposes and calculate travel pay

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

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

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

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

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

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

The VA 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
- Claims processing and production

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

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

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

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

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?
Principle of Use Limitation: Is the use of information contained in the facilities relevant to the mission of the project?

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

The controls in place to assure 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 personnel examine all areas within the facility to ensure information is being appropriately used and controlled.

Data such as patient wait times, provider case load, and VA employee time and attendance is used to perform operational tracking and trending.

Individual users are given access to Veteran's data through the issuance of a user ID and password and using a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user's user ID limits the access to only the information required to enable the user to complete their job. Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.

Section 3. Retention of Information

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

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

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

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

The Area Denver Boundary itself, does not retain information.

- Age
- Biometrics
- Certificate/License numbers
- Contractor Mailing Address
- Contractor Name
- Contractor Personal Telephone Number
- Criminal background information

- Current Medications
- Date of Birth
- Date of Service
- Death certificate information
- Demographics
- Dental Eligibility
- Disclosure requestor information
- Education Information
- Electronic Protected Health Information (ePHI)
- Eligibility Date
- Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Employment information
- Fax Number
- Financial Account Information
- Gender
- Guardian Information
- Health Insurance Beneficiary Account Numbers
- Internal control Number
- International Code Designator (ICD), diagnosis codes
- Internet Protocol (IP) Address Numbers
- Mailing Address
- Medical Record Number
- Member ID
- Military history/service connection
- Mother's Maiden Name
- Name
- Next of Kin
- Other Health Insurance (OHI)
- Phone Number(s)
- Place of Service
- Previous Medical Records
- Procedure Codes/Coded Billing
- Race/Ethnicity
- Referral
- Rendering Provider Zip Code
- Service-connected disabilities
- Social Security Number
- Social Work Assessment/Electronic Protected Health Information (ePHI)
- Tax Identification Number (TIN)

- Tumor PII/PHI statistics
- VA Employee Name
- VA Login Identification (ID)
- Vehicle License Plate Number
- Veteran dependent information
- Zip Code

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. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your Area Boundary may have a different retention period than medical records or education records held within your Area Boundary, please be sure to list each of these retention periods.

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

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

Length of Retention Table

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	***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

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	*Length of Retention*
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.
HAC	VHA RCS 10-1 1260- Care in Community, Health and Medical Care Program, VA, Temporary. Destroy 6 years after all individuals in the record become ineligible for program benefits. VHA RCS 10-1 4000- Financial Management and Reporting Records, 4000.1b: Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting. Temporary. Destroy 6 years after final payment or

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	*Length of Retention*
	cancellation, but longer retention is authorized if required for business use.

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the Area Boundary owner.
This question is related to privacy control DM-2, Data Retention and Disposal.

Retention Schedule Table

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	*Retention Schedule*	*Retention Schedule Link*
VHA	RCS 10-1 RCS 005-1	https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf
VBA	VB-1	https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc
HAC	VHA RCS 10-1	https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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 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)

Additionally, Area Denver follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents **as well as** FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization. In addition, Area Denver follows Department of Veterans Affairs VA Directive 6371, (April 8, 2014), 6500.1.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the **Department of Veterans' Affairs Directive 6500 VA Cybersecurity Program (January 23, 2019)**. When required, this data is deleted from their file location and then permanently deleted from

the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Directive 6500. Digital media is shredded or sent out for destruction per VA Directive 6500. https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1254&FType=2
Paper records are shredded on-site by a shredding company, witnessed by the Records Management Officer, and are accompanied by a certificate of destruction. Non-paper records maintained on magnetic media are destroyed by erasing the magnetic media using an approved software to digitally overwrite the media. The media is then shredded on-site by the contracted shredding company, witnessed by the Records Management Officer per VBA Directive 6300.

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

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

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

HAC –

- Training: Call Center representatives 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. Types of data used by VBA include limited data sets, with mock information (no live claims data) or de-identified information, with all PII removed. This training utilizes approved and controlled access to the Veterans Benefits Management System (VBMS) in "Demonstration Mode", which contains dummy information and is not connected to live claims information. Additionally, live claims information is not presented in recorded environments; PII is not exposed to non-VA personnel. All training access is documented using controlled access with a unique student number and pseudo-claim number assigned.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains

information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the Area Boundary.

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII 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. 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 area to ensure their respective programs are understood and followed by all to protect sensitive information form the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning the proper handling of information.

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).

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

List the Program Office or IT Area Boundary information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT Area Boundary***	***List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary***	***Describe the method of transmittal***	***Provide name of Applicable Area Sites***
VBMS	Filing benefit claims	Social Security Number, Benefits Information, Claims Decision, DD-214	Compensation and Pension Record Interchange (CAPRI) electronic software package	VBA
VistA	Electronic Health Record	Area Boundary Log files, sample clinical data that may contain Protected Health Information (PHI)	Electronically pulled from VistA thru Computerized Patient Record	VBA
Veterans Health Administration (VHA)	Determine eligibility for Veteran compensation.	Name: Social Security Number: Date of Birth: Mailing Address: Zip Code: Phone Numbers:	Electronic transmission methods in accordance with VA	VBA

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
		Email Address: Emergency Contact Information: Financial Account Information: Health Insurance Beneficiary Numbers Current Medications: Previous Medical Records:	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.	
Veterans Health Administration	IAM Access Services System (IAM AcS)	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	Secured accounts provided by IAM integration services.	HAC
Veterans Health Administration	Active Directory Service Accounts	VA Contractors: name, personal mailing address, personal phone number (s)	VA Network	HAC
Veterans Health Administration	Alpha II Adjudication engine	Patient's date of birth and rendering service zip code	A windows service, secured SOAP synchronous XML exchange	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
Veterans 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	HAC
Veterans Health Administration	Austin Automation Center	Payee Name, Address, Zip Code, Payment amount, and canned notes about decisions made	Secure FTPS FIPS 140-2 Secure Transmission	HAC
Veterans Health Administration	Banking Info (BI),	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	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
Veterans 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.	HAC
Veterans 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	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
		Provider Remit to Address		
Veterans 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	HAC
Veterans Health Administration	Community Care Referrals and Authorization System (CCRA)	Referral, Patient information, Social Security Number (SSN), Individual Control Number (ICN), Date of Birth (DOB), First Name, Last Name, Gender, Pre-Authorization information	Secure data transfer via file share using a drop zone behind the VA firewall.	HAC
Veterans Health Administration	Community Care Reimbursement System (CCRS)	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), emergency Contact, Information, Health Insurance (Beneficiary	Via secure file transfer protocol within the VA network, files at rest will be encrypted, CCRA consumes the	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
		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	information CCRS provides	
Veterans Benefits Administration	Compensation and Pension Record Interchange (CAPRI)	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	Compensation and Pension Record Interchange (CAPRI) electronic software package	HAC
Veterans Health Administration	Computerized Patient Record System (CPRS)	Social Security Number	CPRS uses the Auto Hotkey feature provided by Consult Toolbox to send the SSN via webAPI	HAC
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	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)	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
		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	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, 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)	Agent Electronically enters information related the customers call.	HAC
Veterans Health Administration	Data Access Service (DAS)	Name, Social Security Number, Date of Birth, Mailing Address, Zip	Data coming from VA network to the CCRA solution will traverse	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
		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	the VA trusted Internet connection (TIC), arriving at the Cloud Service Router (CSR) in the Veterans Affairs Enterprise Cloud (VAEC); data will then progress to the CCRA cloud via a virtual private network (VPN) connection	
Veterans Health Administration	DEEPSEE	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	Internal VA Access, VA Network utilizing Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2) encryption.	HAC
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	Workflow system. Information is attached to a ticket in PCDUO and assigned to a team for review.	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
		numbers, and date of Birth (DOB)		
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 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)	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)	HAC
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	Electronically pulled and pushed. Secure FTPS FIPS 140-2 Secure Transmission VIA VA network	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
		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		
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 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	HAC
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)	HAC
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	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
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 (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.	Via secure file transfer protocol within the VA network, FIPS 2.0	HAC
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,	Via secure file transfer protocol within the VA network, FIPS 2.0	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
		Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.		
Veteran Health Administration	HAC VistA Drug File	No PII. It's a drug database	No VA network connection, VA employee Query	HAC
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 Medications, Previous Medical Records	No VA network connection, VA employee Query	HAC
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	HAC
Veteran Health Administration Office of	Health Care Claims Processing Eligibility	Patient specific SPI	Simple Object Access Protocol (SOAP) Secured SOAP	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
Community Care -Health Administration Center (HAC) all Veteran Affairs (VA) Medical Centers	and Enrollment Service (HCP EE)		synchronous XML exchange to webservice.	
Veteran Health Administration	Health Data Repository (HDR)	VistA Consults, VistA Appointments, VistA Notes, VistA Postings, VistA Orders	Encrypted electronic transmission (web service)	HAC
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	HAC
Veteran Health Administration	Identity and Access Management (IAM) SSOi	Authentication information as provided by SSOi	Security Assertion Markup Language (SAML) assertion passed as part of a redirect to our page CCRA consumes the info, SSOi provides	HAC
Veteran Health Administration	Interactive Voice Repository (IVR)	Claims status, Payments, Eligibility, SSN, DOB, DOS	Java Database Connection	HAC
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	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	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
		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		
Veteran Health Administration	Office of the Inspector General (OIG)	Social Security Number (SSN), First Name, Last Name, Middle Initial (if provided). Date of Birth (DOB), Gender	Secure email, fax, PowerPoint presentations, word documents	HAC
Veteran Health Administration	OM FSC IPPS (Invoice) Payment Processing System)	Social Security Number (SSN), First Name, Last Name, Middle Initial (if provided). Date of Birth (DOB), Gender	CCRS: The transmission to CDW might happen thru PIT and not directly from CCRS, this still needs to be defined.	HAC
Veterans Health Administration	One Consult Toolbox	Patient's ICN, Name, Address, Zip Code, Phone Number, Email, Social Security Number, and Date of Birth, CAN Score	Consult Toolbox is an Auto Hotkey Application for maintaining CPRS/VistA consult records. Toolbox sends SSN in request to API to retrieve CAN Score. Toolbox gets CAN Score response from CDW which contains PHI/PII via webAPI.	HAC
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	Secure log-in through OCC developed application (FPPS) Austin Automation Center to Submit Payment to Treasury	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
		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		
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	HAC
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 a	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
			service zone behind the VA firewall.	
Veteran Health Administration Austin Information and Technology Center (AITC)	Purchase Care Program Integrity Tool (PIT)	Individual Control Number (ICN), Social Security Number (SSN), Date of Birth (DOB), First Name, Last Name Gender, Medical Procedure Information	Secure data transfer via Windows file share using a drop zone behind the VA firewall, integration of data into PIT.	HAC
Veterans Health Administration	Rightfax	Name, Social Security Number (SSN), Date of Birth (DOB), Mailing address, zip code, Phone number, Fax number, Email address.	Fax and ePrescribing contract.	HAC
Veterans 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.	HAC
Veterans Health Administration	Stellent	Personally Identifiable Information (PII), Personal Health Information (PHI)	Claim Submission forms pulled off the Stellent system.	HAC
Veteran Health Administration / VA Medical Centers	VAMC State Home Per Diem Offices	Name, Social Security Number, Date of Birth, Address, Gender, Age, Health Data, social Work Assessment, Medications	VPN / IPSEC tunnel as required by VA administrators to be installed on Linux Servers.	HAC
Veteran Health Administration	Veterans Information Systems and Technology Architecture (VISTA)	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	Via secure file Transfer protocol within the VA network, FIPS 2.0/ Electronically pulled Off the HAC VistA System/Health Level 7 (HL7) messages from VistA; DST: Electronically pulled from VistA thru	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
		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, clinical service, urgency	Computerized Patient Record System (CPRS)	
Veteran Health Administration	VistA Fee Basis (FB), Austin Automation Center	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.	HAC
Veteran Health Administration	VLER Data Access Services (DAS)	Referral Number, Date of Service, National Provider Identifier (NPI)	CCRA: Secure data transfer via Windows file share using a drop zone behind the VA firewall, with subsequent, secure Extract Transform Load (ETL)	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
			Integration of data into CCRS.	
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.	HAC
Veterans Health Administration	Debt Management Center (DMC)	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI)	MoveIT software	HAC
Veterans Health Administration	Move it	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	Moveit application	HAC

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
		Physical Address, Provider Remit to Address		
Veterans Health Administration	Veterans Information Solution (VIS)	Name, Social Security Number, Date of Birth, Address, Health Insurance Beneficiary Numbers Account Numbers, Previous Medical Records, Veteran Service-Connected Status and Conditions.	Electronically (through email, SharePoint)	HAC
Veterans Benefits Management System (VBMS)	Investigation of Fraud, Waste, and Abuse and possible prosecution of beneficiary and/or provider	Name, Social Security Number, Date of Birth, Address, Health Insurance Beneficiary Numbers Account Numbers, Previous Medical Records, Veteran Service-Connected Status and Conditions.	Electronically (through email, SharePoint)	HAC
Veteran Health Administration	Death/burial benefit	Death certificates, veteran eligibility	Hard copy mailing	ECH
Denver VAMC's Veteran Centers	Continuity of care, eligibility,	Read only access to health information for plan of treatments.	Electronically reviewed thru Computerized Patient Record System (CPRS)	ECH
VA Tumor Register	Tracking & trending of diseases	Diagnosis & procedures, tumor status, treatment outcome, survivor tracking, type of treatments, demographics, hormone, radiation, chemotherapy, problem lists	Electronic tumor register package	ECH
Veterans Choice Program (Veterans Access, Choice	Tracking & trending of disease progression	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable	Secure web portal	ECH

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
and Accountability Act of 2014)		Information (III) appropriate to the agreement.		
VA Health Eligibility Center	Determine veteran eligibility	Service dates, SSAN, demographics, service connection	Scanned documents uploaded into shared software program	ECH
Consolidated Patient Account Center	Medical care cost recovery	Diagnosis, service connection, dates of service, health insurance information, demographics,	Electronically pulled from VistA thru Computerized Patient Record System (CPRS); Huron system extracts data from systems	ECH
VA Network Authorization office – NON-VA Care Coordination (NVCC)	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	ECH
Veterans 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	ECH
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.	ECH
DAS – listed in PTA	Health PHI/PII pertinent to veterans and benefits	Personally Identifiable Information (PII), Protected Health Information (PHI), Individually Identifiable	SOAP over HTTPS using SSL encryption and Certificate exchange	ECH

List the Program Office or IT Area Boundary information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT Area Boundary*	*Describe the method of transmittal*	*Provide name of Applicable Area Sites*
		Information (III), System Log files, sample clinical data that may contain Protected Health Information (PHI)		

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT Area Boundary information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary***	***List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***	***List names of Applicable Area Sites***
Social Security Administration	Eligibility for Federal benefits	SSN, Name, Address	National ISA/ MOU	Site to Site (S2S), IPSEC Tunnel, Secure FTP	VBA/HAC/ECH
Internal Revenue Services	Income verification	Name, Financial Information	ISA/ MOU, Computer Matching Agreement	Secure Web-Portal, Secure Socket Layer	VBA/HAC/ECH
DPRIS Department of Defense	Determine military service dates, eligibility	Name, Service Information, SSN	MOU	Bi-directional Health Information Exchange	VBA

List External Program Office or IT Area Boundary information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
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	HAC
Cognosante Military Veteran Health (MVH), Limited Liability Company (LLC) - HSRM COTS	data management, information technology and support services for home	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s),	Contract, BAA, ISA/MOU	Data is shared with external providers via HTTPS, Data	HAC

List External Program Office or IT Area Boundary information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
	telehealth platforms	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		includes the minimum information specific to the referral	
Amazon Web Service (AWS) GovCloud - AWS GovCloud		Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Emergency Contact, Information, Health Insurance (Beneficiary Numbers, Account Numbers), Current	Business Associate Agreement (BAA)	TIC-VPN	HAC

List External Program Office or IT Area Boundary information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
		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			
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	Contract and BAA (PC3 only)	Via a representational state transfer Web service over HTTPS, CCRA consumes the information TriWest Provides; TLS, SFTP, Azure Express Route (encrypted)	HAC

List External Program Office or IT Area Boundary information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
		(whether the individual is a Veteran or spouse of a Veteran), Contact Notes (additional information regarding, contacting the patient), Preauthorization, Service-Connected Disability			
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 (SEOC), SEOC Description, Facility Name, Average Wait Time, Average Drive Time, Electronic Data Interchange Personal Identifier (EDIPI)	Contract, MOU, MOA, ISA	Secure Web-Portal, Secure Socket Layer SSL/TLS	HAC

List External Program Office or IT Area Boundary information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
Optum - Optum (Contractor)	Coordinates patient care services in the community	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)	HAC
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	MOU	Via secure file transfer protocol within the VA	HAC

List External Program Office or IT Area Boundary information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
		Numbers/Account Numbers, Current Medications, Provider's TIN and Address information.		network, paper, and/or by phone.	
Department of Defense (DOD)		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.	HAC
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	Contract, ISA/MOU	Secure FTPS FIPS 140-2 Secure Transmissio n	HAC

List External Program Office or IT Area Boundary information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
		Numbers, Internet Protocol (IP) Address Numbers, Previous Medical Records, and Veteran Service-Connected Status and Conditions			
Office of the Inspector General (OIG) - Office of the Inspector General (OIG) Legal Demand	Fraud Waste and 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 Transmissio n or UPS, or Fax	HAC
Office of Finance - Office of Finance- Improper Payments Elimination and Recovery Improvement Act (IPERIA)	Recovery Audit contract to recoup overpayments 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	MOU	Secure FTPS FIPS 140-2 Secure Transmissio n or UPS, or Fax	HAC

List External Program Office or IT Area Boundary information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
		Numbers, Internet Protocol (IP) Address Numbers, Previous Medical Records, and Veteran Service-Connected Status and Conditions			
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) 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	Contract	Electronically pulled and pushed. Secure FTPS FIPS 140-2 Secure Transmission VIA VA network	HAC
Conduent Federal Solutions system - Conduent, system Burgess	Claims pricing services	Social Security Number, Zip Code, Veteran's diagnosis code, Procedure Codes),	Contract, National Business Associate	Web portal	HAC

List External Program Office or IT Area Boundary information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
Reimbursement System (BRS)		and Individually Identifiable Information (III).	Agreement, ISA/MOU		
HMS Federal - In-Sync (subcontractor to HMS Federal)	Recovery Audit contract to recoup overpayments and under payments made to the VA	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI)	Business Associate Agreement (BAA)	Subcontractor enters contractor environment	HAC
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	ECH
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	ECH
Colorado State Department of Health; Death Certificates Office: via Electronic Death Registration System (EDRS)	Medical Records	Name, Date of Birth, Sex, SSN, demographics, health information	Local Agreement with Decedent Affairs	Via secure web portal	ECH
University of Colorado, Denver (UC Denver)	The purpose of this interconnection between the Department of Veterans Affairs (VA) Eastern Colorado Health Care System (ECHCS) and	Name, Date of Birth, Sex, SSN, demographics, health information	Local ISA/MOU	Business Partner Gateway – VA TIC Gateway via a S2S VPN tunnel connection. Protected through the	ECH

List External Program Office or IT Area Boundary information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
	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.			use of FIPS 140-2	
Minuteman Technology Services	The purpose of the connection is to establish a bi-directional 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.	First Name, Last Name, Middle Name o Veteran ID (or other unique identifier) o Indicator for whether person was living at the end of FY 2017 (or most recent FY available) o Full Address, State name, County name of residence o Urbanicity (urban/rural) o Urbanicity (urban/large rural/small rural/isolated)	Local ISA/MOU	Via Secure File Transfer Protocol (SFTP), using port 22, and using FIPS approved, 256-bit encryption	ECH

List External Program Office or IT Area Boundary information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
		o Telephone Number o Email Address o Date of Birth o Gender o Ethnicity o Race o Transition Status o Maximum separation date o Veteran Status o VHA usage information o Years of service o Retirement Indicator o Branch, Rank o Wars served in o Character of Service o Components served in o Branch of most recent separation o Benefits used o Benefits used 2 years prior to most recent year available o Benefits used 1 year prior to most recent year available o Active health insurance o An index of whether or not the veteran is deemed competent enough			

List External Program Office or IT Area Boundary information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT Area Boundary*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT Area Boundary*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
		to receive his/her payments directly or whether they must be paid to a fiduciary o Unemployment status o Household income			

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

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

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

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

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

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

Privacy Risk: The sharing of data is necessary for individuals to receive benefits at 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 Area Boundary that their information has been collected and is

being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

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

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 SOR) in the Federal Register and online. An online copy of the SOR can be found at: https://www.oprm.va.gov/docs/CurrentSORList_4_29_20.pdf

Applicable SORs

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	***Applicable SORs***
VHA	• Non-VA Fee Basis Records-VA, SOR 23VA10NB3 • Patient Medical Records-VA, SOR 24VA10P2 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA12 • Community Placement Program-VA, SOR 65VA122 • Health Care Provider Credentialing and Privileging Records-VA¸SOR 77VA10E2E • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10P2 • Income Verification Records-VA, SOR 89VA10NB • Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA13 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10D • National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147VA10NF1 • VHA Corporate Data Warehouse- VA 172VA10P2 • Applicants for Employment under Title 38, USC-VA, SORN 02VA135 • Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attendings, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records-VA, SORN 14VA05 (Nov. 18, 2010) • Patient Medical Records-VA, SORN 24VA19 (Nov 19, 2009) • Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA, SORN 34VA12 (May 27, 2010) • Community Placement Program-VA, SORN 65VA122 • Health Care provider credentialing and Privileging Records-VA¸SORN 77VA10Q (March 26, 2008)

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	*Applicable SORs*
	• Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SORN 79VA10P2 (Oct. 31, 2012, as amended) • Income Verification Records-VA, SORN 89VA19 (May 8, 2008) • Automated Safety Incident Surveillance and Tracking System-VA, SORN 99VA13 (March 31, 2009) • Telephone Service for Clinical Care Records- VA, SORN 113VA112 (May 8, 2009) • The Revenue Program Billings and Collection Records-VA, SORN 114VA16 (Dec. 10, 2009, as amended) • National Patient Databases-VA, SORN 121VA19 (May 11, 2012, as amended) • Patient Advocate tracking System (PATS)-VA, SORN 100VA10NS10 • Compliance Records, Response, and Resolution of reports of Persons Allegedly Involved in Compliance Violations-VA, SORN 106VA17 • Community Residential Care and Medical Foster Home Program-VA, SORN 142VA114 • Employee Medical Files System Records-VA, SORN Title 5: OPM/GOVT-10 • Employee Medical File System Records (Title 38)-VA, SORN 08VAO5 • Police and Security Records-VA, SORN 103VAO7B • 54VA10NB3, ‘‘Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files-VA’’ (March 3. 2015) • 55VA10NB, Customer Relationship Management System (CRMS) • 43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records-VA
VBA	• Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28
HAC	• 23VA10NB3 Non-VA Fee Basis Records-VA, • 24VA10P2 Patient Medical Records-VA, • 77VA10E2E Health Care Provider Credentialing and Privileging Records-VA • 79VA10P2Veterans Health Information Systems and Technology Architecture (VistA) Records-VA • 114VA10D The Revenue Program Billings and Collection Records-VA • 121VA10A7 National Patient Databases-VA • 147VA10NF1 Enrollment and Eligibility Records-VA • 172VA10P2 VHA Corporate Data Warehouse- VA • 54VA10NB3, ‘‘Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files-VA’’ (March 3. 2015) • 55VA10NB, Customer Relationship Management System (CRMS)

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	*Applicable SORs*
	• 43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records-VA

This Privacy Impact Assessment (PIA) also serves as notice of 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 to all enrolled & eligible Veterans receiving VHA healthcare whenever changes to the document is made. The current version from VHA is dated effective 30 September 2019.

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

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

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

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

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

The Area 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-DEN/HAC-VHA/ECH-VHA	***Information Consent Rights***
VHA	Individuals have the right to consent to particular uses of information. Individuals are directed to use the Request for Authorization to Release Medical Records Form (VA Form 10-5345) describing what information is to be sent out and to whom it is being sent to. 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 the facility Release of Information office 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 Release of Information office 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 at http://benefits.va.gov/benefits/offices.asp
HAC	Individuals have the right to consent to particular uses of information. Individuals are directed to use the Request for Authorization to Release Medical Records Form (VA Form 10-5345) describing what information is to be sent out and to whom it is being sent to. 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 the facility Release of Information office for review and processing. Individuals may also request to Opt-Out

Site Type: VBA-DEN/HAC-VHA/ECH-VHA	*Information Consent Rights*
	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 Release of Information office to obtain information.

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 at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the facilities within the Area Boundary are exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).
If the facilities within the Area Boundary are not a Privacy Act Area Boundary, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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 http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf.

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

As directed in VA SOR Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28(July 19, 2012), individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. A list of regional VA offices may be found at: http://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 area Release of Information Office where care is received.

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

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

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

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

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 myHealthevet can use the system to review their VHA health records. Any information a veteran identifies in their records as being inaccurate, incomplete, irrelevant &/or untimely can be addressed through the amendment process by contacting the ECH Privacy Officers at VHAECHPrivacy@va.gov

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

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

Mitigation: Area 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 received in September 2019 and when newly enrolled for VHA healthcare. 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 SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 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. They can be contacted at either 720.857.5980 or VHAECHROI@va.gov for assistance.

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

Section 8. Technical Access and Security

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

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

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

Identify users from other agencies who may have access to the Area Boundary and under what roles these individuals have access to the Area Boundary. Who establishes the criteria for what PII can be shared? Describe the different roles in general terms that have been created to provide access to the Area Boundary. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

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

Individuals receive access to Area Denver by gainful employment in the VA or upon being awarded a contract that requires access to the Area systems. Upon employment, the Office of Information & Technology (OI&T) creates computer and network access accounts as determined by employment positions assigned. Users are not assigned to software packages or network connections that are not part of their assigned duties or within their assigned work area. 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 Area Boundary (ePAS). Users submit access requests based on need to know and job duties. Supervisor, ISSO and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need to know basis.

Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel. Access to computer rooms at 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 r (ISSO), local Area Manager, System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

Human Resources notify Divisions, IT and ISSO of new hires and their start date(s), 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 Area Boundary and the PII? If yes, what involvement will contractors have with the design and maintenance of the Area Boundary? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the Area Boundary?

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

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

Contractors will have access to the Area Boundary after completing the VA Privacy and Information Security Awareness training and Rules of Behavior annually, and after the initiation of a background investigation. Contractors are only allowed access for the duration of the contract this is reviewed by the privacy officer and the designated Contracting Officer Representative (COR). Per the National Contractor Access Program (NCAP) guidelines, contractors can have access to the Area Boundary only after completing mandatory information security and privacy training, Privacy and HIPAA Focused Training as well as having completed a Special Agency Check, finger printing and having the appropriate background investigation scheduled with Office of Personnel Management. Certification that this training has been completed by all contractors must be provided to the employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy. Contractors with Area Denver access must have an approved computer access request on file. The area manager, or designee, in conjunction with the area ISSO and the applicable COR reviews accounts for compliance with account management requirements. User accounts are reviewed periodically in accordance with National schedules.

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

VA offers privacy and security training. Each program or Area Boundary may offer training specific to the program or Area Boundary that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All 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 area Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officers also perform subject specific trainings on an as needed basis.

Each site identifies personnel with significant information system security roles and responsibilities. (i.e., management, system managers, system administrators, contracting staff,

HR staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained. The Talent Management System offers the following applicable privacy courses:

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

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

If Yes, provide:

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

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

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

Authorization and Accreditation has been completed for the Area Denver boundary.

System Name: Area Denver
System ID: 781
System Acronym: 554

1. Date the Authority to Operate (ATO) was granted, 13-May-2019
2. ATO with Conditions, ATO extension due to COVID-19 priorities and activities
3. The amount of time the ATO was granted for, authorization length 522 days
4. The FIPS 199 classification of the system (MODERATE)

Section 9. References

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

ID	Privacy Controls
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System 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	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Privacy Officers

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

Robert V McGinn 1394631

Digitally signed by Robert V McGinn 1394631
Date: 2021.07.15 08:07:25 -06'00'

Privacy Officer, Robert McGinn

Dana E. Krishland 3499286

Digitally signed by Dana E. Krishland 3499286
Date: 2021.07.15 08:18:05 -06'00'

Privacy Officer, Dana Krishland

JULIE C. DRAKE 969177

Digitally signed by JULIE C. DRAKE 969177
Date: 2021.07.15 09:55:43 -06'00'

Privacy Officer, Julie Drake

Daniel W. Quigley 170662

Digitally signed by Daniel W. Quigley 170662
Date: 2021.07.15 07:18:43 -06'00'

Privacy Officer, Daniel Quigley

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.

Nichelle R Downing 271709

Digitally signed by Nichelle R Downing 271709
Date: 2021.07.15 07:48:12 -06'00'

Information System Security Officer, Nichelle R. Downing

Ashton Q Botts 671895

Digitally signed by Ashton Q Botts 671895
Date: 2021.07.15 09:14:05 -06'00'

Information System Security Officer, Ashton Botts

EDUARDO A LORENZO 177164

Digitally signed by EDUARDO A LORENZO 177164
Date: 2021.07.15 12:20:14 -06'00'

Information System Security Officer, Eduardo Lorenzo

DEETTA S. CHAGNON 584665

Digitally signed by DEETTA S. CHAGNON 584665
Date: 2021.07.15 12:25:50 -06'00'

Information System Security Officer, DeEtta Chagnon

Signature of Area Manager

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

JAMES M. HUGHES 182665

Digitally signed by JAMES M. HUGHES 182665
Date: 2021.07.19 15:06:43 -06'00'

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-DEN/HAC-VHA/ECH-VHA	***Applicable NOPPs***
VHA	**Notice of Privacy Practices:** https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147 **VHA Privacy and Release of Information:** https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3233
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 their 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** https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf

APPENDIX B – PII Mapped to Components

PII Mapped to Components Table

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
Server 1:	Yes	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Current Medications, Previous Medical Records, Tax Identification Number (TIN), Member ID	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	HAC
Server 2:	Yes	Yes	Yes	Name, Social Security Number (SSN), Member	The data is utilized to positively identify the	AES256, Behind VA Firewall,	HAC

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				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,	Veteran and/or beneficiary.	Hard disks are encrypted.	

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this compone nt store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
Server 3:	Yes	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Emergency Contact Information, Current Medications, Previous Medical Records, Tax Identification Number (TIN), Member ID	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	HAC
Server 4:	Yes	Yes	Yes	Name, Social Security Number	The data is utilized to positively identify the	AES256, Behind VA	HAC

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				(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	Veteran and/or beneficiary.	Firewall, Hard disks are encrypted.	

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
Server 5:	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 Billing Information, Health	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	HAC

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this compone nt store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				Information, Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
Server 6:	Yes	Yes	Yes	Name, social security number, date of birth, mailing address, zip code, phone numbers, email address, fax, current medications, Previous Medical Records/biometrics, Provider name, provider	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	HAC

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				address, provider telephone number, National Provider Identifier (NPI), financial information			
Server 7:	Yes	Yes	Yes	Name, social security number, date of birth, mailing address, zip code, phone numbers, email address, fax, current medications, Previous Medical Records/biometrics, Provider name, provider address, provider telephone number, National Provider Identifier (NPI), financial information	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	HAC

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this compone nt store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
Server 8:	Yes	Yes	Yes	Name, social security number, date of birth, mailing address, zip code, phone numbers, email address, fax, current medications, Previous Medical Records/biometrics, Provider name, provider address, provider telephone number, National Provider Identifier (NPI), financial information	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	HAC
Server 9:	Yes	Yes	Yes	Veteran/Beneficiary: Name, Social Security Number, telephone number, member Identification Number, address, email, health	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	HAC

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				information, financial information, biometrics. Provider: Name, Business name, Address, Telephone, National Provider Identifier (NPI), financial information			
Server 10:	Yes	Yes	Yes	Name, social security number, date of birth, mailing address, zip code, phone numbers, current medications, Previous Medical Records/biometrics, Provider name, provider address, provider telephone number, National Provider	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	HAC

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				Identifier (NPI), financial information			
Server 1-A:	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 Billing Information, Health Information, Prescription Information,	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this compone nt store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
Server 2-A:	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	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				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 3-A:	Yes	Yes	Yes	Name, Social Security Number (SSN), Member Identification Number, Patient Control Number, Medical Record	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				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			

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				associate Veteran with Beneficiary.			
Server 4-A:	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 Billing Information, Health Information, Prescription Information, Procedure Codes	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
Server 5-A:	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	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this compone nt store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				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 6-A:	No	No	No				ECH
Server 7-A:	No	No	No				ECH
Server 8-A:	No	No	No				ECH
Server 9-A:	Yes	Yes	Yes	Name, Social Security Number (SSN), Member Identification Number, Patient	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this compone nt store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				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		are encrypted.	

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				Beneficiary Information to associate Veteran with Beneficiary.			
Server 10-A:	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 Billing Information, Health Information, Prescription	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this compone nt store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
Server 11:		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	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this compone nt store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				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.			
Server 12:	Yes	Yes	Yes	Name, social security number, date of birth, mailing address, zip code, phone numbers, email	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				address, fax, current medications, Previous Medical Records/biometrics, Provider name, provider address, provider telephone number, National Provider Identifier (NPI), financial information			
Server 13:	Yes	Yes	Yes	Name, social security number, date of birth, mailing address, zip code, phone numbers, email address, fax, current medications, Previous Medical Records/biometrics, Provider name, provider address, provider	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				telephone number, National Provider Identifier (NPI), financial information			
Server 14:	Yes	Yes	Yes	Name, social security number, date of birth, mailing address, zip code, phone numbers, email address, fax, current medications, Previous Medical Records/biometrics, Provider name, provider address, provider telephone number, National Provider Identifier (NPI), financial information	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	ECH
Server 15:	Yes	Yes	Yes	Disability/Compensation Social	The data is utilized to positively identify the	AES256, Behind VA	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this compone nt store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				Security Number, Benefits Information, Claims Decision, DD-214	Veteran and/or beneficiary.	Firewall, Hard disks are encrypted.	
Server 16:	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 Billing Information, Health Information,	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this compone nt store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				Prescription Information, Procedure Codes Number, Veteran and Provider Tax Identification Number (TIN), Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
Server 17:	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),	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				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.			
Server 18:	No	No	No				ECH
Server 19:	No	No	No				ECH
Server 20:	Yes	Yes	Yes	Name, Social Security Number (SSN), Member	The data is utilized to positively identify the	AES256, Behind VA Firewall,	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				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),	Veteran and/or beneficiary.	Hard disks are encrypted.	

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				Current Medications, Health Insurance Beneficiary Information to associate Veteran with Beneficiary.			
Server 21:	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 Billing Information,	The data is utilized to positively identify the Veteran and/or beneficiary.	AES256, Behind VA Firewall, Hard disks are encrypted.	ECH

Components of the Area Boundary collecting/storing PII	*Does this component collect PII? (Yes/No)*	*Does this component store PII? (Yes/No)*	*Does this component share, receive, and/or transmit PII? (Yes/No)*	*Type of PII (SSN, DOB, etc.)*	*Reason for Collection/ Storage of PII*	*Safeguards*	*Provide Names of Applicable Sites*
				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.			