April 19, 2021

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

AREA PHILADELPHIA
NORTH ATLANIC DISTRICT ONE

Facilities Supported by the Area

Facilities Supported by the Area:
1. Corporal Michael J. Crescenz VAMC and its 5 CBOCS Gloucester, Burlington, Camden, West Philadelphia and Saracini
2. Philadelphia Regional Office
3. VA Insurance Center
4. Philadelphia National Cemetery Administration `Philadelphia NCA, Beverly NCA, Finn's Point NCA

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

Area Boundary Contacts:

Area Privacy Officer

Name	Phone Number	Email Address	Location
Designated Area PO (The PO located in the same VAMC as the Area Manager): Celita Rivera	215 823 5800 X 204438	Celita.Rivera@va.gov	CMCVAMC
Ondreya Barksdale	215 823 5800 X 204377	Ondreya.Barksdale@va.gov	CMCVAMC
Amy Kinsley	215 842 2000 X 2554	Amy.Kinsley@va.gov	VBA Regional Office PO
Lakisha Wright	202 632 7216	Lakisha.Wright@va.gov	NCA, VA Central Office PO
Chiquita Dixson	202 873 5196	Chiquita.Dixson@va.gov	Insurance Center PO

Area Information System Security Officer

Name	Phone Number	Email Address	Location
Designated Area ISSO: (The ISSO located in the same VAMC as the Area Manager): Anupam Anand	215 823 5800 X 205159	Anupam.Anand@va.gov	CMCVAMC
Mike Yung	215 823 5800 X 205159	Mike.Yung@va.gov	CMCVAMC
Richard Powell	215 823 5800	Richard.Powell@va.gov	Insurance Center
Harry Guynup	215 842 2000 X 4276	Harry.Guynup@va.gov	Regional Office

Name	Phone Number	Email Address	**Location**
Genea Belton	215 842 2000 X 4814	Genea.Belton@va.gov	Regional Office

Area Manager

Name	**Phone Number**	**Email Address**	**Location**
Georgia T David	215 823 4376	Georgia.David@va.gov	CMCVAMC

Abstract

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

Area Philadelphia is an Information Area Boundary that consists of Corporal Michael J Crescenz VAMC, Camden CBOC, Burlington CBOC, Gloucester CBOC, Victor J Saracini CBOC, West Philadelphia CBOC, Bristol Veterans Center, Arch Veterans Center, Onley Veterans Center, Norristown Veterans Center, Snyder House RRTP, Administration Annex, Dow Building, Multiservice Center, Regional Benefits Office, VA Insurance Center (to include the locally managed application VICTARS), National Cemetery Administration, Washington Crossing National Cemetery, Beverly Cemetery. 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 Philadelphia is an Information Area Boundary that consists of Corporal Michael J Crescenz VAMC, Camden CBOC, Burlington CBOC, Gloucester CBOC, Victor J Saracini CBOC, West Philadelphia CBOC, Bristol Veterans Center, Arch Veterans Center, Onley Veterans Center, Norristown Veterans Center, Snyder House RRTP, Administration Annex, Dow Building, Multiservice Center, Regional Benefits Office, VA Insurance Center , (to include the locally managed application VICTARS) National Cemetery Administration, Washington Crossing National Cemetery, Beverly Cemetery. 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.

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, Insurance Payment System (IPS), Electronic Insurance (EIN), LIPAS Life Insurance Policy Administration etc. There are individual PIAs that contain detailed information on the maintenance, dissemination and sharing practices, and storage of the PII/PHI for each Enterprise system accessed by the facilities.

Any external information sharing conducted by the facilities within the Area Boundary. The Area is sharing /receiving information with the Social Security Administration, Department of Defense, and other external Systems listed in 5.1. A citation of legal authority to operate the Area Boundary can be found in 1.6 for example, "The Area operates under Health Insurance Portability and Accountability Act of 1966 (HIPSS) Privacy Act of 1974, Veterans Benefit Administration comes from 38 U.S,Code Chapter 77, as well as other authorities listed in 1.6.

The Area is using the VA Enterprise Cloud System (VAEC) which is outside of the Area boundary. Further information can be found in the VAEC PIA.

The completion of this PIA will not result in circumstances that require changes to business processes.

The applicable SORs for *Philadelphia* include:

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	***Applicable SORs***
*VHA	• Non-VA Fee Basis Records-VA, SOR 23VA10NB3 • Patient Medical Records-VA, SOR 24VA10A7 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 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 79VA10. • Income Verification Records-VA, SOR 89VA10NB • Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA13 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10D • National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147VA10NF1 • VHA Corporate Data Warehouse- VA 172VA10P2
^VBA	• Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28
/NCA	• Veterans and Dependents National Cemetery Gravesite Reservation Records -VA SOR 41VA41 • Veterans and Dependents National Cemetery Interment Records-VA SOR 42VA41 • VA National Cemetery Pre-Need Eligibility Determination Records -VA SOR 175VA41A
Insurance Center	• Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance — 36VA29 (October 22, 2010); in the Federal Register (75 FR 65405)

Section 1. Characterization of the Information

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

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

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

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

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

☒ 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)

The CMCVAMC Area Philadelphia also collects uses, disseminates, creates, or maintains the following

Birth Sex
• Gender
• Next of Kin
• Medical Records of Non-VA Providers
• Diagnosis of Disease; Treatment notes; Prescribed medications; Laboratory results; Problem lists of ongoing persistent medical needs; Reports of Radiology procedures; Surgical

Procedures; Historical health information in the form a Health History and Discharge Summaries from inpatient hospitalization.

• Guardian Information
• Electronic Protected Health Information (ePHI)
• Tumor PII/PHI
• Self-Identified Gender Identity

• Military History/Service Connection
• Service-connected disabilities
• Employment information
• Disclosure requestor information
• Veteran dependent information
• Death certificate Information
• Criminal background information
• Education information

PII Mapping of Components

Philadelphia consists of 6 servers and 65 databases. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected within Philadelphia 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 Philadelphia 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). Department of U.S. Treasury, Office of Service members Group Life Insurance (SGLI) State and local agencies, and local courts. Accredited Veterans Service Organizations (VSO) and other organizations aiding veterans and members of uniformed services; VA-approved claims agents]

Criminal background information is obtained from Electronic Questionnaires for Investigations Processing (E-QIP) and National Crime Information Center (NCIC) and used to confirm employment and/or volunteer eligibility and to assist the VA Police Service while conducting internal investigations.

^ Additional sources include:

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

1.3 How is the information collected?

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.

The CMCVAMC Medical Center) collects most information including contact information, medical history, insurance , and financial data directly from the veterans' for benefits and enrollment using paper forms (such as the enrollment form for VA health care) or interviews and assessments with the individual. Information about military service history and service used to confirm an individual's eligibility for VA Services is obtained directly from the Department of Defense (DoD) and the Veterans Benefits Administration (VBA). The DoD provides military records, including medical records compiled when the

patient was a member of the US Military. The VBA provides records which include the type and percentage of granted 'service-connected' disabilities, the dates of service-connected disability ratings, and, in some cases, the VBA populates patient demographics to the Area Philadelphia in order to provide a Compensation and Pension examination to a claimant. These outside records are transmitted through a secure shared computer linkage.
The VBA also provides a toll-free number for Veterans, 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 sued 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 benefit.

The VA Insurance Center collects electronic data as described above and including:

• Retired pay allotments (DFAS, U.S. Coast Guard) and deductions from benefits (Hines VAITC). The data is collected specifically to start, stop, or change payments for VA Insurance.
• Data interchange with Social Security Administration (SSA) is done to request and receive addresses, or a date of death. The Insurance Center receives this data via VA's Hines data center.
• Data interchange with Department of Defense (DFAS) – to process allotments from military retired pay to pay premiums.
• Data interchange with VAITC, Hines, Illinois – to process deductions from benefits (DFB) to pay premiums; to receive address changes for veterans who elect this method to pay; to receive Notice of Death (NOD).
• Data interchange with Department of Treasury – to process disbursements and returned items. This data is received in Philadelphia over a dedicated line from Treasury that utilizes their approved encryption.
• Data interchange with the Veterans Affairs DoD Identity Repository (VADIR) - to identify military personnel who have been medically retired with a service disability of 50% (DoD disability) or higher so they can be contacted. This data is received in Philadelphia via the Office of Servicemembers' Group Life Insurance at Prudential Insurance Company. We also receive veterans' Specially Adapted Housing (SAH) information form the Austin data center which is used in conjunction with the VMLI program.

Means of Collection Table

Site Type: VBA/VHA/NCA or Program Office	***Means of Collection***
*VHA	Information collected directly from patients, employees and/or other members of the public is collected using paper forms (such as the VA Form 10-10EZ enrollment form for VA health care), or interviews and assessments with the individual. Other information provided by veterans such as address and phone number, next of kin and emergency contact information, and similar information. Additionally, Veterans medical recorded by a doctor or other medical providers.

Site Type: VBA/VHA/NCA or Program Office	*Means of Collection*
^VBA	There are many VA forms used by Veterans to apply for and/or adjust 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.
/NCA	MEM does not receive information electronically from other systems. Information is collected through direct phone calls to the NCSO or A long-term plan is in place for the Pre-Need system to transmit data electronically to the EOAS component of BOSS, but these activities are currently processed by scheduling office personnel. Documents from funeral homes, next of kin, and other points of contact from the decedent are sent to scheduling office personnel and uploaded into BOSS. AMAS processes approximately 360,000 claims for standard government headstones or markers (VA Form 40-1330) and Monument and Presidential Memorial Certificate Request (VA Form 40-0247) applications annually. Data from the forms are manually entered into the system. Forms and supporting documentation required to verify memorial benefits eligibility, such as the DD214, are scanned/uploaded.
VA Insurance Center	Insurance information subject to the Paperwork Reduction Act: • VA MATIC Change/Changes to Bank, Checking Account (VA Form 29-0165, OMB Control #2900- 0525) • Direct Deposit Enrollment or Change (VA Form 29-0309, OMB Control # 2900-0665) Designation of Beneficiary (VA Form 29-336, OMB Control # 2900-0020) Application for Reinstatement (VA Form 29-352, OMB Control # 2900-0011) • Application for Reinstatement—Non-medical, Comparative Health (VA Form 29-353, OMB Control # 2900-0011) • Claim for Disability Insurance Benefits (VA Form 29-357, OMB Control # 2900-0016) • Certificate Showing Residence and Heirs of Deceased Veteran or Beneficiary (VA Form 29-541, OMB Control # 2900-0469) • Insurance Deduction Authorization (VA Form 29-888, OMB Control # 2900-0024)

Site Type: VBA/VHA/NCA or Program Office	*Means of Collection*
	• Application for Cash Surrender Value (VA Form 29-1546, Page 1, OMB Control # 2900-0012) • Application for Policy Loan (VA Form 29-1546, Page 2, OMB Control # 2900-0012) • Application for Change of Permanent Plan/Medical (VA Form 29-1549, OMB Control # 2900-0179) • Claim for One Sum Payment (VA Form 29-4125 OMB Control # 2900-0060) • Claim for Monthly Installments (NSLI) (VA Form 29-4125a, OMB Control # 2900-0060) • Application for Service-Disabled Veterans Insurance (VA Form 29-4364, OMB Control # 2900-0068) • Application for Supplemental Service-Disabled Veterans Insurance (VA Form 29-0188, OMB Control # 2900-0539) • Veterans' Mortgage Life Insurance Statement (VA Form 29-8636, OMB Control # 2900- 0212)

Information related to an employee's employment application may be gathered from the applicant for employment, which is provided to an application processing website, USA Jobs.

Information from outside resources comes to the *Philadelphia* using several methods including *Secure* Web Portals, Secure VPN Connection, Email, facsimile, and paper documents. Chief among these sources, are the DoD, SSA, and IRS. The DoD provides military records, including medical records compiled when the patient was a member of the US Military. Income information is verified using information from the Social Security Administration (SSA) and the Internal Revenue Service (IRS).

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

Include a statement of why the 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 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 *Philadelphia* are as varied as the types of information collected.

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

Purpose of Information Collection Table

Site Type: VBA/VHA/NCA or Program Office	***Purpose of Information Collection***
*VHA	• To determine eligibility for health care and continuity of care • Emergency contact information is cases of emergency situations such as medical emergencies • Provide medical care • 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 • Research
^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.
/NCA	• MEM collects and maintains information to verify the identity and eligibility of the Veteran or decedent for burial and monument services.
VA Insurance Center	• To provide for the provision of coverage to eligible service members and veterans, as well as to provide for the payment of insurance benefits to the proper beneficiary.

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.

For the CMCVAMC Medical Center-Much of the information provided by veterans or other members of the public, such as address and phone number, next of kin and emergency contact information, and similar information are assumed to be accurate because it is provided directly by the individual. Additionally, information entered an individual's medical record by a doctor or other medical staff is also assumed to be accurate and is not verified.

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

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

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

List the full legal authority for operating the Area 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

Legal Authority Table

Site Type: VBA/VHA/NCA or Program Office	Legal Authority
*VHA	• Veterans' Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a) • Health Insurance Portability and Accountability Act of 1996 (HIPAA) • Privacy Act of 1974 • Freedom of Information Act (FOIA) 5 USC 552 • VHA Directive 1605.01 Privacy & Release of Information • VA Directive 6500 Managing Information Security Risk: VA Information Security Program.
^VBA	• Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b) • 38 U.S.C 77 • Title 10 U.S.C Chapter 106a, 510,1606 and 1607 • Section 501(a) and Chapters 11,13,15,18,23,30,31,32, 33,34,35,36,39,51,53 and 55.
/NCA	• Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(a), 501(b), and Chapter 24, Sections 2400-2404.
VA Insurance Center	• 38 U.S.C. §§ 1901 – 1989. • 38 U.S.C. § 5701. • 5 U.S.C. § 552a; • 38 CFR §§ 1.500 – 1.527; and • 83 FR 44407 (Insurance system of records notice)

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 *Philadelphia* 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 *Philadelphia* 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.

- **Name**: Used to identify the patient during appointments and in other forms of communication
- **Social Security Number**: Used as a patient identifier and as a resource for verifying income Information with the Social Security Administration
- **Date of Birth**: Used to identify age and confirm patient identity
- **Mother's Maiden Name:** Used to confirm patient identity
- **Mailing Address**: Used for communication, billing purposes and calculate travel pay
- **Zip Code**: Used for communication, billing purposes, and to calculate travel pay
- **Phone Number(s):** Used for communication, confirmation of appointments and conduct Telehealth appointments
- **Fax Number**: used to send forms of communication and records to business contacts, Insurance companies and health care providers
- **Email Address**: used for communication and 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.
- **Financial Account Information:** Used to calculate co-payments and VA health care benefit eligibility
- **Health Insurance Beneficiary Account Numbers**: Used to communicate and bill third part Health care plans
- **Certificate/License numbers**: Used to track and verify legal authority to practice medicine and Licensure for health care workers in an area of expertise.
- **Internet Protocol (IP) Address Numbers**: Used for configuration and network connections. Network Communication allows information to be transferred from one Information Technology System to another.
- **Current Medications**: Used within the medical records for health care purposes/treatment, prescribing medications, and allergy interactions.
- **Previous Medical Records**: Used for continuity of health care
- **Race/Ethnicity**: Used for patient demographic information and for indicators of ethnicity-related diseases.
- **Next of Kin**: Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
- **Guardian Information**: Used when patient is unable to make decisions for themselves.
- **Electronic Protected Health Information (ePHI):** Used for history of health care treatment, during treatment and plan of treatment when necessary.
- **Military history/service connection**: Used to evaluate medical conditions that could be related to location of military time served. It is also used to determine VA benefit and health care eligibility.
- **Service-connected disabilities**: Used to determine VA health care eligibility and treatment plans/programs
- **Employment information**: Used to determine VA employment eligibility and for veteran contact, financial verification.

- **Veteran dependent information**: Used to determine benefit support and as an emergency contact person.
- **Disclosure requestor information**: Used to track and account for patient medical records released to requestors.
- **Death certificate information**: Used to determine date, location, and cause of death.
- **Criminal background information**: Used to determine employment eligibility and during VA Police investigations.
- **Education Information**: Used for demographic background information for patients and as a determining factor for VA employment in areas of expertise. Basic educational background, e.g. High School Diploma, college degree credentials
- **Gender**: Used as patient demographic, identity, and indicator for type of medical care/provider and medical tests required for individual.
- **Tumor PII/PHI Statistics**: Used to evaluate medical conditions and determine treatment plan

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

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

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 *Philadelphia CMC VAMC* uses statistics and analysis to create general reports that provide the VA a better understanding of *[patient care, benefits, services provided and to improve veteran experience.* 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.
4. Analyze veteran experience and satisfaction.

These reports may track:

- The number of patients enrolled, provider capacity, staffing ratio, new primary care patient wait time, etc. for Veterans established with a Patient Care Aligned Team (PACT)
- Beneficiary travel summary/benefits
- Workload and cost resources for various services, i.e., mental health, primary care, home dialysis, fee services, etc.
- Daily bed management activity
- Coding averages for outpatient/inpatient encounters
- Satisfaction of Healthcare Experience of Patients (SHEP) data as it pertains to customer satisfaction regarding outpatient/inpatient services
- Unique patient trends
- Clinic wait times

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

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

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or 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 personal examine all areas within the facility to ensure information is being appropriately used and controlled.

• All employees with access to a veteran's information are required to complete the VA Privacy and Information Security awareness training and Rules of Behavior annually and additionally the Privacy and HIPAA Training TMS 10203 for the CMC VA Medical Center employees.

• Access to the VA system is requested through the approved automated account request process. Account access is reviewed and approved by employee supervisor and designated OIT staff. Information access levels are determined by each employees' risk level and duties.

• Individual users are given access to a 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-related duties.

• The Insurance Center System of Records Notice (SORN), also known as the Veterans and Uniformed Services Personnel Programs of US Government Life Insurance—VA (36VA29), available at Federal Register at 75 FR 65405 and online at https://www.oprm.va.gov/privacy/privacy_SOR.aspx provides a detailed explanation of the ways information is collected and used based on the mission of the VA Insurance Center.

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 *Philadelphia* Boundary itself, does not retain information.

- Name

- Previous medical records
- Social Security Number (SSN)
- Race/ethnicity
- Date of Birth
- Next of Kin
- Mother's Maiden Name
- Guardian Information
- Mailing Address
- ePHI
- Zip Code
- Military history/service connection
- Phone Numbers
- Service connection disabilities
- Fax Numbers
- Employment information
- Email address
- Veteran dependent information
- Emergency contact info
- Disclosure requestor information
- Financial account information
- Death certification information
- Health insurance beneficiary account numbers
- Tumor PII/PHI statistics
- Certificate/license numbers
- Criminal background investigation
- Internet Protocol address numbers
- Education Information
- Current medications
- Gender

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

Site Type: VBA/VHA/NCA or Program Office	*Length of Retention*
	• Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA. • Education electronic folders are retained at the servicing Regional Processing Office. Education folders may be destroyed in accordance with the times set forth in the Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA. • Employee productivity records are maintained for two years after which they are destroyed by shredding.
/NCA	• Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(a), 501(b), and Chapter 24, Sections 2400-2404.
VA Insurance Center…	• Hardcopy records are retained and disposed of in accordance with disposition authorization approved by the Archivist of the United States. • VICTARS, the primary records storage and retrieval system for the insurance programs, maintains imaged insurance records indefinitely through the Facility Insurance Center GSS. Hardcopy records imaged into VICTARS are stored for 31 days prior to destruction. Original copies of imaged beneficiary designation documents are stored indefinitely at the NARA Mid Atlantic Regional Center. • Computerized records accessible through ITS are also maintained indefinitely through the Facility Insurance Center GSS. • Back-up VA ITC archive records are stored on tape for one year prior to being erased or written over.

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

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

Retention Schedule Table

Site Type: VBA/VHA/NCA or Program Office	***Retention Schedule***
*VHA	Records Control Schedule 10-1 Records Control Schedule 005-1
^VBA	Records Control Schedule VB-1 Part 1, Section, XIII, Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc
/NCA	Veterans (Deceased) Headstone or Marker Records-VA SORN 48VA40B: Retained indefinitely
VA Insurance Center	Records Control Schedule VB-1 Part 1, Section, XIII, Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII

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

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.?

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

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

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

^ Paper records are shredded on-site by a shredding company, witnessed by the Records Management Officer, and are accompanied by a certificate of destruction. Services at VHA can use CD shredders located throughout the medical center. If there is media w Services.

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

Yes, where feasible to minimize the risk to privacy using PII for research, testing, or training:
When feasible, the Area Philadelphia uses a test account and pseudo patients for research, testing, or training purposes. VHA Directive 1906 Data Quality Requirements for Healthcare Identity Management describes the requirements for using test patient information. Examples include "ZZ Test Patient One" with a pseudo SSN of "000-00-0000."

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 *Philadelphia* 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, *Philadelphia* adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as

described in question 3.4. The Area *Philadelphia* ensures that all personnel involved with the collection, use and retention of data are trained in the correct process for collecting, using, and retaining this data. A Records Management Officer (RMO), Privacy Officer (PO) and an Information System Security Officer (ISSO) are assigned to the area to ensure their respective programs are understood and followed by all to protect sensitive information form the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning the proper handling of information.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. 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*
Veterans' Health Administration (VistA)	Veterans' Health Administration (VistA) Medical Diagnosis, and treatment Sharing	System Log files, clinical data that may contain protected health information including medical diagnosis, and documentation of medical care and medication.	Electronically pulled from VistA thru Computerized Patient Record System (CPRS)	VHA
Veterans Benefit Administration (VBA) Compensation and Pension Interchange (CAPRI) Determine eligibility for Veteran compensation.	Determine the eligibility for compensation and pension	Name, social security number, date of birth, demographic information, medical record	Compensation and Pension Record Interchange (CAPRI) electronic software package	Philadelphia Regional Office
VA/OGC Department of Veteran Affairs General Counsel Office	Share Agency Legal defense and Appeals	Name, social security number, demographic information, medical records, incident reports, risk management, or quality assurance related information / and any discovery Case files requested for litigation, settlement, or appeal	Electronic, Mail delivery (USPS/UPS/FedEx)	VHA
VA National Cemetery Administration (NCA).	Determine Benefits for Deceased Veterans of NCA Burial Services and plots in military cemeteries.	Veteran's name, SSN, character of service, DD214, death certificates, veteran eligibility Veteran's name, SSN, character of service, DD214, death certificates, veteran eligibility	Electronic mail delivery, facsimile	NCA
Veterans' Health Administration Health Eligibility Center (HEC)	Enrollment and Master Patient Index	Name, Date of Birth, Sex, SSN, demographics, and health information	Enrollment Systems Redesign or automatic upload to HEC via Vista Automatic Upload	VHA
Veterans Affairs (VA) VA Research	Research Studies	Name, Social Security Number, DOB Mail and Email Address, Phone Numbers, Emergency Contact	Information may be transmitted upon request in an electronic, verbal format based on the individual request	VHA

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, Current medications, Previous Medical Records and Race/Ethnicity as appropriate to the request		
VA Cancer Registry (VACCR)	Identification and Outcome Tracking of cancer patients	Name, SSN, DOB, Address Telephone Phone numbers. Diagnosis and procedures, tumor status, treatment outcome, survivor tracking, type of treatments, demographics, problem lists	Electronic tumor registry package	VHA/
VA HIV Registry	HIV Registry cases	Name, SSN, DOB. Diagnosis and procedures, HIV/AIDS status, treatment outcomes, survivor tracking, type of treatments, demographics, problem lists	Electronic HIV registry package	VHA/
VA Network Authorization Office- Non-VA Care Payments- Medical Payment of Non-VA Care	Health/ Medical Payment Authorization	Name, SSN, DOB, Address Phone numbers. diagnoses, medical history, service connection, provider orders, VHA recommendation/approval for non-VA care.	Fee basis claim system (FBCS) authorization software program	VHA
VHA Veterans Center	To share medical information/ demographics, Medical history, service connection, provider orders with community providers	Name, SSN, DOB, Address Phone numbers, read only access to health information for treatment planning and support services.	Electronically viewed through CPRS	VHA
VBA Continuity of Care	networked Non-VA Health Care	Name, SSN, DOB, Address Phone numbers. Medical History, Diagnoses, providers' orders, medications, prognosis, and care	Electronic via EDI interface/ paper via US postal service	VBA
VA Virtual Lifetime Electronic Record /	/ Medical treatment Information for Continuity of Care	To share medical information/Demographics, diagnoses, medical history, service connection, provider orders, with community providers.	Electronic via EDI interface/ paper via US postal service	VHA

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 Insurance Center 116 Insurance Products Division	VBA Insurance Center employees to administer life insurance benefits for Veterans and Beneficiaries.	Insurance System data—Names, addresses, and claim numbers. Personally, Identifiable Information (PII) SSN, Address, Date of Birth	LAN, WAN	VA Insurance Center
Veterans Benefits Affairs Insurance Center (VICTARS)	VBA Insurance Center employees to administer life insurance benefits for Veterans and Beneficiaries.	VMLI Deduction Insurance data – Names and claim numbers. Personally, Identifiable Information (PII) SSN, Address, Date of Birth	LAN, WAN	VA Insurance Center
/Veterans Benefits Affairs/ Regional Office- Share T- 11-	SHARE 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 and Social Security Administration	Social Security Number, date of birth, mailing address, contact information, Veteran demographic information, VA benefit information	Compensation and Pension Record Interchange (CAPRI) electronic software package	Philadelphia Regional Office
Veterans Benefit Administration Centralized Administrative Accounting Transaction (CAATS)	Determine eligibility for compensation and pension benefits.	Social Security Number, date of birth, mailing address, contact information, Veteran demographic information, medical diagnosis, treatment, and care records	Sends encrypted data from VAAUSCATWEB20 via SFTP. This data is destroyed after transmission. CAATS retrieves the completed data via SFTP. Data is destroyed after retrieval.	VBA
Veterans Benefits Administration (VBA) Veterans Information System (VIS)	An inquiry tool that provides a consolidated view of comprehensive eligibility and benefits utilization data from across VBA and DoD	Social Security Number, date of birth, mailing address, contact information, Veteran demographic information, medical diagnosis, treatment, and care records	Sent securely over internet using FIPS 140-2 secure connection	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***
Veterans Benefits Administration /Exam Management System (EMS)	Determine eligibility for compensation and pension benefits.	Social Security Number, date of birth, mailing address, contact information, Veteran demographic information, medical diagnosis, treatment, and care records	Sends encrypted data from VAAUSCATWEB20 via SFTP.	VBA
Veterans Affairs Time and Attendance System (VA) Time and Attendance VATAS	Time and Attendance	Employee Name, leave and attendance balances	SOAP over HTTPS using SSL encryption and Certificate Exchange	VA
Veterans Benefits Administration Customer Relationship Management/ Unified Desktop (CRM/UD)	Provides status on veterans/ beneficiaries claims and updates to systems	Name, demographic, and diagnosis and treatment information for customer service management	SOAP over HTTPS using SSL encryption and certificate exchange	VBA
Veterans Benefit /Veterans Benefits Management System (VBMS)	Determine eligibility for compensation and pension benefits.	Social Security Number, date of birth, Veteran demographic information, medical diagnosis, treatment, VA benefit information, banking information, mailing address, phone number, email address, dependent information	Electronic transmission methods through Hines Citrix Gateway.	VBA
VA Insurance Center /281 Austin Information Technology Center (ITC) and VA-DOD Identity Insurance/Repository (VADIR)	There are three (3) purposes: 1) to inform veterans of VGLI availability. 2) To ensure veterans do not have an excess of $400,000 of SGLI and VGLI. 3) To identify disabled Veterans with a 50% or greater military disability rating to	Files of recently discharged non- disabled and disabled veterans. Files of veterans with VGLI coverage., Personally Identifiable Information (PII)	Connect Direct	VA Insurance Center

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*
	conduct outreach on insurance benefits. This information is sent directly to Prudential Insurance Company of America, which is supervised by the Insurance Center			
VA Insurance Center /282 Hines ITC	The purpose is to process changes to insureds' addresses, and process premiums deducted from benefits.	Personally, Identifiable Information (PII) SSN, Address, Date of Birth	Connect Direct	VA Insurance Center

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 *Philadelphia Area Boundary*. 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 can 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*
SSA - Social Security Administration	Veteran Social Security Benefit determination	Personally, Identifiable Information and III including SSN, Name, Address to assist determine Veteran's Social Security Disability	National ISA/ MOU	Site to Site (S2S), IPSEC Tunnel, Secure FTP	CMCVAMC
DoD - Department of Defense	E health exchange health and benefit information between DOD and VA	PII/SPI may include prescriptions, allergies, illnesses, Lab and radiology results, immunizations, past medical procedures, clinical notes	National ISA/MOU; Title 38 USC-VA, SORN 02VA135	Bi-directional Health Information Exchange	CMCVAMC
State Reporting/ United States Department of Health and Human Services (DHHS)	For public protection, (PHI), and Individually Identifiable Information	Pertinent Personally Identifiable Information (PII), Protected Health Information to include name, demographic and diagnosis information	Standing Letter PA Safety Code	Facsimile	CMCVAMC
PA State Department of Health City of Philadelphia	For public health and protection of the all citizens	Pertinent Protected Health information to include the name, address, and medical diagnosis	Standing Letters	Facsimile	CMCVAMC
Internal Revenue Service (IRS)	Eligibility Verification	Name, address, income information	National ISA/ MOU	Secure Web Portal	CMCVAMC
Food and Drug Administration	State reporting of required schedule medications	Name, address, medication prescription name and frequency filled	National ISA/MOU	Site to Site (S2S) VPN Tunnel	CMCVAMC

State Prescription Monitoring Program	State reporting of required schedule medications	Name, address, medication prescription name and frequency filled	National Directive	Site to Site (S2S) VPN Tunnel	CMCVAMC
Local/State Law Enforcement Agencies/ PA State Police,	Requirement of mandated reporting by law enforcement. PII data is used to identify the patient in the system and between systems	Name, Address, Social Security Number, charges, subpoenas, warrants.	Title 38, U.S.C, Sections 501(b) and 304; SORN VA 24VA10P2	National Crime Information Data Base and through facsimile	CMCVAMC
Local, State, & Federal Government Agencies; Other Medical Institutions	Continuity of Care to obtain non-VA- Medical Services	Local, State, & Federal Government Agencies; Other Medical Institutions to include the name, demographic, and Medical treatment, diagnosis and medications, Social Security Numbers.	Title 38, U.S.C, Sections 501(b) and 304; SORN VA 24VA10P2	Electronic, Facsimile	CMCVAMC
Office of Personnel Management	Employment.	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), Including Resume, reference, background check status, Names, Social Security Number, and demographic information	National ISA/MOU	Electronic, written, or verbal format based on the individual request. Secure facsimile or hard copies via routine mail.	CMCVAMC
Transcriptions Inc. DBA Alpha Transcriptions, INC.	Medical Transcription Service	Name, Last four, medical history, diagnosis, principal medical diagnosis, prognosis and discharge diagnosis and medications	National ISA/MOU	Secured VPN	CMCVAMC
Health Net Federal Services	Continuity of Care for Choice Visits	Name, Last four, medical history, diagnosis, principal medical diagnosis, prognosis and discharge diagnosis and medications	National ISA/MOU	Secure Facsimile	CMCVAMC
Medical Examiner	Cause of Death Determination	Name, Last four, medical history, diagnosis, principal	National Directive 1605.01	Secure Facsimile	CMCVAMC

		medical diagnosis, prognosis and discharge diagnosis and medications related to cause of death			
OLYMPUS	Identification of Patient between systems	(Patient name, SSN, DOB) The data is used to identify the patient in the system and between systems	ISA/MOU	VPN Tunnel	CMCVAMC
SCRIPTPRO	Outpatient Pharmacy Prescription filling	Patient Name, SSN, DOB	National ISA/MOU	Site to Site(S2S) VPN Tunnel	CMCVAMC
Omnicell	Patient Medical Administration	Patient Name, SSN, DOB, diagnoses, and medications	National ISA/MOU	Site to Site (S2S) VPN Tunnel	CMCVAMC
LabCorp	Patient Lab Administration	Patient Name, SSN, DOB, diagnoses	National ISA/MOU	Site to Site (S2S) VPN Tunnel	CMCVAMC
VA Federal Health Care Center (FHCC)	VA DOD health care exchange	Patient Name, SSN, DOB, diagnoses, Pertinent Personally Identifiable Information and Pertinent Health Information	National ISA/MOU	Site to Site (S2S) VPN Tunnel	CMCVAMC
ROCHE Diagnostics	Laboratory Medical Diagnostics	Patient Name, SSN, DOB, diagnoses, Pertinent Personally Identifiable Information and Pertinent Health Information	National ISA/MOU	Site to Site (S2S) VPN Tunnel	CMCVAMC
Philadelphia City Police	Assist with Missing persons, and warrants	Patient Name, DOB, Address, telephone number	MOU	Secure Fax, verbally over the telephone	CMCVAMC
National Crime Information	Police verification of criminal information;	Pertinent PII which may include Veteran Name, DOB, Address, telephone Number, Diagnosis Information	National ISA/MOU	Site to Site(S2S) VPN Tunnel	CMCVAMC
Gift of Life PA	Organ Donating Procurement	Patient Name, DOB, Pertinent Diagnosis Information for banking of cadaveric organs, eyes, or tissues	Local MOU;45 CFR164.512	Verbally via phone call	CMCVAMC
Electronic Questionnaire for Investigations (E- QIP)	Employment Investigations	Pertinent Personally Identifiable Information which includes Employee Name, DOB, Address, SSN, telephone	National ISA/MOU	Site to Site (S2S) VPN Tunnel	CNVAMC

		Number, Resumes, References			
Shredding Services -Land Shark shredding, LLC/Titan	Data Destruction Services for temporary records and those eligible for final destruction under VHA RCS 10-1	Copies of Medical Records that could include Patients Name, Date of Birth, Social Security Number, Address, Medical Diagnosis, and Treatment. Any Copies VA sensitive records such as drafts.	National ISA/MOU	Hard copies of the Certificate of Destruction are sent after final destruction	CMCVAMC
National Veterans Service Organizations Such as Veterans of Foreign War9 VFW) etc.	Treatment Planning, Veteran Assistance with Services	Name, Social Security Number, Date of Birth, Mailing Address, Phone Numbers, email addresses, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers, Current Medications. Previous Medical Records and Race/ Ethnicity as appropriate to the request	Title 38 Code of Federal Regulations (CFR) s14.633, Privacy Act HIPAA Privacy Rule Power of Attorney (POA)	Electronically, verbally, or written in a sentence format. For example, information may be transmitted upon request in an electronic written or verbal format based on the individual request	CMCVAMC
Third Party Insurance Agencies	VMLI Deduction Insurance Data-Verification	Social Security Number, date of birth, mailing address, contact information, Veteran demographic	BAA, VA Claims Confidentiality Statue 38 USC 5701	Electronic Data Interchange (EDI)	CMCVAMC
PA and NJ Department of Child Protective Services	Reporting suspected Child Abuse	Pertinent PII including Name, date of Birth address, telephone number, clinical medical information, as well as similar contact information for the victim	Standing Letters	Telephone	CMCVAMC
Department of Aging	Reporting abuse of elders.	Pertinent PII including Name, date of Birth address, telephone number, clinical medical information, as well as similar contact information for the alleged abuser	Standing Letters	Telephone	CMCVAMC

Phillips	. Bed Label Information	Sends waves forms and numeric to PICIS at each bedside	National ISA/ MOU	VPN Connection	
U.S. Bank	Insurance Policy Information	Name, VA INS File number, financial information, Insurance Policy Information	Local ISA/MOU	One – Way VPN Connection	Insurance Center
VBA Medical Support LOS Angelas (MILSA	Determine eligibility for Veteran compensation and pension.	Social Security Number, benefits Information, Claims Decisions DD-21	National ISA/MOU	Sent securely over internet using FIPS 140-2 secure connection	VBA
VBA Logistics Health Incorporate D(LHI)	Determine eligibility for Veteran compensation and pension.	Social Security Number, date of birth, mailing address, contact information, Veteran demographic information, medical diagnosis, treatment, and care records	National ISA/MOU	Sent securely over internet using FIPS 140-2 secure connection	VBA
VETFED	Determine eligibility for Veteran compensation and pension.	Social Security Number, date of birth, mailing address, contact information, Veteran demographic information, medical diagnosis, treatment, and care records	National ISA/MOU	Sent securely over internet using FIPS 140-2 secure connection	VBA
Defense Personnel Records Information Retrieval (DPRIS)	The Defense Personnel Records Information Retrieval System (DPRIS) is an electronic gateway that allows authorized users to access the Services' Official Military Personnel File (OMPF) and Joint Services Records Research Center (JSRRC Military) Information to include severance and retirement pay	Social Security Number, date of birth, mailing address, contact information, Veteran demographic information, medical diagnosis, treatment, and care records	National ISA/MOU	Data from the DFAS to VA will be encrypted and transferred using Connect: Direct Secure Plus File Transfer software through a VA Transport Layer Protocol site-to- site VPN tunnel, which provides FIPS 140-2 compliant	VBA
Quality Timeliness and	Determine eligibility for Veteran compensation and pension.	Social Security Number, date of birth, mailing address, contact	National ISA/MOU	Sent securely over internet using FIPS	VBA

Customer Service (QTC)		information, Veteran demographic information, medical diagnosis, treatment, and care records		140-2 secure connection	
Veterans Evaluation Services (VES)	Medical Disability Examinations	Name, Date of Birth, Social Security, Address, Telephone Number, Medical Diagnosis and Disability Claims Information	National ISA/MOU	Sent securely over internet using FIPS 140-2 secure connection	VBA
Defense Accounting System (DFAS)	Payroll	System Log files, sample clinical data that may contain Protected Health Information (PHI)	National ISA/MOU	Data from the DFAS to VA will be encrypted and transferred using Connect: Direct	VBA

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 the *[Philadelphia Area Boundary]*. 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.

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

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	***Applicable SORs***
*VHA	• Non-VA Fee Basis Records-VA, SOR 23VA10NB3 • Patient Medical Records-VA, SOR 24VA10A7 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 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 79VA10 • Income Verification Records-VA, SOR 89VA10NB • Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA131 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10D • National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147-VA10NF1 • VHA Corporate Data Warehouse- VA 172VA10P2
^VBA	• Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28
/NCA	• Veterans and Dependents National Cemetery Gravesite Reservation Records -VA SOR 41VA41 • Veterans and Dependents National Cemetery Interment Records-VA SOR 42VA41 • VA National Cemetery Pre-Need Eligibility Determination Records -VA SOR 175VA41A

VA Insurance Center	• Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance — 36VA29

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

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

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

Employees and contractors are required to review, sign, and abide by the VA information security and privacy rules of behavior Rules of Behavior and Privacy/HIPAA training on an annual basis. For contractors COR is responsible for keeping ROB on file for that contract.

The Insurance Center also provides notice by publishing the VA System of Record Notice (SORN), also known as the Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance — 36VA29 (October 22, 2010); in the Federal Register (75 FR 65405) and online. An online copy of the SORN can be located at https://www.oprm.va.gov/privacy/privacy_SOR.aspx

This Privacy Impact Assessment (PIA) also serves as notice of the Area Boundary As required by the eGovernment Act of 2002, Public Law 107-347208(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".

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 *Philadelphia* 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 *the VHA Veteran Health Administration , Veteran Benefits and Insurance, or the National ,VBA, OR NCA, National Cemetery Administration OPM and to the respective Human Resources Components to obtain and maintain employment.*

6.3 Do individuals have the right to consent to uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?
This question is related to privacy control IP-1, Consent

Information Consent Rights Table

Site Type: VBA/VHA/NCA or Program Office	***Information Consent Rights***
*VHA	Yes. Individuals must submit in writing to their facility PO. The request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, no information on the individual is given out. Individuals can request further limitations on other disclosures. A veteran, legal guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer or the appointed social worker 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

Site Type: VBA/VHA/NCA or Program Office	*Information Consent Rights*
	nearest VA regional office, a list of which can be found on the VBA website.
VA Insurance Center	Any individual who wishes to determine whether a record is being maintained in the Insurance System of Records under his or her name or other personal identifier, or who wants to determine the contents of such record, or has a routine inquiry concerning the status of his or her insurance under this system may contact the VA Insurance Center in Philadelphia, Pennsylvania at (215) 381-3029. Requests concerning the specific content of a record must be made in writing or made in person to the VA Insurance Center in Philadelphia, Pennsylvania. The inquirer should provide the full name of the veteran or member of the uniformed services, their insurance file number or VA claim number or social security number, the date of birth of the veteran or member of the uniformed services, and reasonably identify the benefit or system of records involved. If the insurance file number or any of the other identifiers noted above are not available, the service number, and/or location of insurance records that will aid VA personnel in locating the official insurance records should be provided. The Insurance System of Records Notice (SORN) provides that an individual generally must consent to each use of the information in his insurance record; however, the SORN also lists exceptions to when the individual's consent is not required, such exceptions are listed as "routine uses" in the SORN and are clearly identified.

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 *Philadelphia* exists or that it collects, maintains, and/or disseminates PII, PHI or PII/PHI about them.

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

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page to obtain information about FOIA points of contact and information about agency FOIA processes.

If the facilities within the Area Boundary are exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the facilities within the Area Boundary are not a Privacy Act Area Boundary, please explain what procedures 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 Health*e*Vet program, VA's online personal health record. More information about my Health*e*Vet is available at https://www.myhealth.va.gov/index.html.

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

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

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.

The following procedure is from VA Handbook 6300.4:

(1) An individual may request amendment of a record pertaining to themselves contained in a specific VA system of records by mailing or delivering the request to the office concerned. The request must be in writing and must conform to the requirements in paragraph 3b (3) of this handbook. It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requester should be advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired.

(2) Not later than 10 days, excluding Saturdays, Sundays, and legal public holidays, after the date of receipt of a request to amend a record, the VA official concerned will acknowledge in writing such receipt. If a determination has not been made, the acknowledgement will inform the individual when he or she may expect to be advised of action taken on the request. VA will complete a review of the

request to amend or correct a record as soon as reasonably possible, normally within 30 days from receipt of the request (excluding Saturdays, Sundays, and legal public holidays).

(3) Where VA agrees with the individual's request to amend his or her record(s), the requirements of 5 U.S.C. 552a(d) will be followed. The record(s) will be corrected promptly, and the individual will be advised promptly of the correction. Amendment consists of adding information to the record, altering information in the record, or deleting information in the record. Under the Privacy Act, if information is altered or deleted, the previous version must be obliterated and illegible after amendment. The amendment should be annotated "Amended, Privacy Act, (date), (signature and title of amending official)."

(4) If the record has previously been disclosed to any person or agency, and an accounting of the disclosure was made, prior recipients of the record will be informed of the correction. FL 70- 19, Notification to Other Person or Agency of Amendment to a Record, may be used.

(5) If it is determined not to grant all or any portion of the request to amend a record, the official will promptly notify the individual in writing. The individual will be advised of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend. The notice will specify the reason(s) for denying the request, identify the VA regulations or statutes upon which the denial is based, and advise that the denial may be appealed in writing to the General Counsel (024), Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. FL 70-20, Notification of Initial Refusal to Amend a Record under the Privacy Act, may be used for this purpose.

(6) The determination on an appeal will be made not later than 30 days, excluding Saturdays, Sundays, and legal public holidays, from the date the individual's letter of appeal is received unless the Secretary or Deputy Secretary, for good cause shown, extends such 30-day period. If the 30-day period is so extended, the individual will be

notified promptly of the reasons for the extension and the date on which a final determination may be expected. The final determination in such appeals will be made by the General Counsel or Deputy General Counsel.

(7) If the General Counsel or Deputy General Counsel finds that the adverse determination should be reversed, he or she will notify the VA office or station of the remedial action to be taken. The VA office or station will promptly carry out that action. The General Counsel or Deputy General Counsel will promptly notify the individual in writing of the corrective action. The field station or Central Office organization that provided the initial decision will inform previous recipients of the record that a correction has been made.

(8) If the General Counsel or Deputy General Counsel determines that the adverse determination will not be reversed, the individual will be notified promptly in writing of that determination, the reasons therefor, and of his or her right to seek judicial review of the decision pursuant to section 3 of the Privacy Act (5 U.S.C.

(9) If the adverse determination is sustained by the General Counsel or Deputy General Counsel, the individual will also be advised promptly of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend. The statement may contain information that the individual believes should be substituted.

(10) When an individual files a statement disagreeing with VA's decision not to amend a record, the record will be clearly annotated so that the fact that the record is disputed is apparent to anyone who may subsequently access, use, or disclose it. When the disputed record is disclosed to persons or other agencies, the fact of the dispute will be clearly noted. Copies of the statement of disagreement will be provided, and, when appropriate, copies of a concise statement of VA's reasons for not making the amendment(s) requested will also be provided.

(11) A decision by either the General Counsel or Deputy General Counsel pursuant to paragraph 3f (7) of this handbook is final. It is subject to judicial review in the district court of the United States in which the complainant resides, or has his or her principal place of business, or in which the VA records are located, or in the District of Columbia.

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 seeking an amendment to their medical records will contact the Corporal Michael J. Crescenz Medical Center Privacy Officer.

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

Veterans 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, and Medical Center Veteran Privacy Rights Brochures.

Veterans 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

Veterans' amendment appeal rights are outlined in the Corporal Michael J. Crescenz VA Medical Center Privacy Officer amendment letters as follows.

Office of General Counsel (024)

Department of Veterans Affairs

810 Vermont Avenue, N.W.

Washington, D.C. 20420

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.

Veterans and their beneficiaries are notified of the procedures for correcting their records at the Insurance Center through the VA System of Records Notice (SORN), also known as the Veterans and Uniformed Services Personnel Programs of US Government Life Insurance - 36VA29. Based on the SORN's Records Access Procedure—individuals desiring access to, and who wish to contest information in their VA insurance records and learn more about related procedures should write to the Insurance Center at 5000 Wissahickon Ave, PO Box 8079, Philadelphia, PA 19101.

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 the VHA Privacy Appeal Process outlined in the amendment response letter.,

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 my Healthe*e*Vet can use the system to make direct edits to their health records for any information in the Computerized Medical Record.

Individuals desiring redress or who wish to contest information in, their VA insurance records and learn more about related procedures should write to the Insurance Center at 5000 Wissahickon Ave, PO Box 8079, Philadelphia, PA 19101.

There is no formal redress for records stored in the Philadelphia Regional Office; however, Veterans and other beneficiaries may contact their local VA regional office to learn how to access their VA records and correct, if necessary, the records used by the RO.

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

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

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

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

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

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

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

The *Corporal Michael J. Crescenz VA Medical Center* Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.

The Veterans' Health Administration (VHA) established My HealtheVet 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.

This privacy risk is mitigated at the Insurance Center by information provide in Insurance SORN (Veterans and Uniformed Services Personnel Programs of US Government Life Insurance—36VA29)), Records Access Procedure which states that individuals desiring access to, or wishing to contest information, in their insurance records can write to the Insurance Center at 5000 Wissahickon Ave, PO Box 8079, Philadelphia, PA 19101.

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 the *Philadelphia Area* by gainful employment in the VA or upon being awarded a contract that requires access to the Philadelphia Area information systems. Upon employment, the Office of Information & Technology (OI&T) creates computer and network access accounts as determined by employment positions assigned. Users are not assigned to software packages or network connections that are not part of their assigned duties or within their assigned work area. VA *Philadelphia* area users get access to the information systems using Your IT for network access and EPAS for Vista access. Staff are not allowed to request additional or new access for themselves.

Access is requested utilizing Electronic Permission Access Area Boundary (ePAS) and Security Management System (SMS). Users submit access requests based on need to know and job duties. Supervisor/SAC's, 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 VA Police. Access to computer rooms at VA Philadelphia 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 *Philadelphia* 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 services, IT and ISSO of new hires and their start date(s), either through [*email*] The Division that the person is going start working follows Your IT procedures for network access and EPAS for Vista access.

• 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 Philadelphia Area Boundary after completing the VA Privacy and Information Security Awareness training and Rules of Behavior annually, and after the initiation of a background investigation. Contractors are only allowed access for the duration of the contract this is reviewed by the privacy officer and the designated Contracting Officer Representative (COR). Per the National Contractor Access Program (NCAP) guidelines, contractors can have access to the Area Boundary only after completing mandatory information security and privacy training, Privacy and HIPAA Focused Training as well as having completed a Special Agency Check, finger printing and having the appropriate background investigation scheduled with Office of Personnel Management. Certification that this training has been completed by all contractors must be provided to the employee who is responsible for the contract in question.

In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy. Contractors with VA *Philadelphia* access must have an approved computer access request on file maintained by COR for that contract. 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 VA employees who have access to VA computers must complete the onboarding and annual mandatory Privacy and Information Security Awareness Training, this training educates each employee in the NEO orientation as scheduled by our education department. Contractors, WOC (who self-enroll in TMS) are supposed to complete their training in TMS Prior to being granted system access, all users will either attend Information System Security Officer (ISSO) led training during NEO or complete VA Privacy and Information Security Awareness Training with Rules of Behavior in the Talent Management System (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 and Information Security Officer during new employee orientation a 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.***

The Date the new Area Philadelphia Authorization to Operate (ATO) was granted on 4/7/21 and will expire on April 8, 2022. The Area Philadelphia ATO has a FIPS Classification of Moderate.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Privacy Officers

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

CELITA RIVERA 128006 Digitally signed by CELITA RIVERA 128006
Date: 2021.05.18 14:50:20 -04'00'

Privacy Officer, Celita Rivera

Ondreya R Barksdale 342397 Digitally signed by Ondreya R Barksdale 342397
Date: 2021.05.24 08:20:02 -04'00'

Privacy Officer, Ondreya Barksdale

Amy Kinsley Digitally signed by Amy Kinsley
Date: 2021.05.18 15:41:25 -04'00'

Privacy Officer, Amy Kinsley

LAKISHA V WRIGHT 111646 Digitally signed by LAKISHA V WRIGHT 111646
Date: 2021.05.18 16:09:47 -04'00'

Privacy Officer, Lakisha Wright

Chiquita Dixson 126558 Digitally signed by Chiquita Dixson 126558
Date: 2021.05.18 15:53:55 -04'00'

Privacy Officer, Chiquita Dixson

Signature of Information Security Systems Officers

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

Anupam Anand 404738 Digitally signed by Anupam Anand 404738
Date: 2021.05.18 16:26:30 -04'00'

Information System Security Officer, Anupam Anand

Yung, Mike Digitally signed by Yung, Mike
Date: 2021.05.19 09:16:22 -04'00'

Information System Security Officer, Mike Yung

RICHARD S POWELL 116807 Digitally signed by RICHARD S POWELL 116807
Date: 2021.05.20 06:17:52 -04'00'

Information System Security Officer, Richard Powell

HARRY J GUYNUP 103332 Digitally signed by HARRY J GUYNUP 103332
Date: 2021.05.19 08:46:28 -04'00'

Information System Security Officer, Harry Guynup

Genea Belton 158619 Digitally signed by Genea Belton 158619
Date: 2021.05.19 07:28:58 -04'00'

Information System Security Officer, Genea Belton

Signature of Area Manager

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

Georgia T. david 409995 Digitally signed by Georgia T. david 409995
Date: 2021.05.18 15:23:42 -04'00'

Area Manager, Georgia David

APPENDIX A – Notice

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

Applicable Notices

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

APPENDIX B – PII Mapped to Components

PII Mapped to Components Table

Components of the Area Boundary collecting/storing PII *(Each row refers to a grouping of databases associated with a single server)*	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Provide Names of Applicable Sites***
Server 1 • Candidate Mailing Output Database • Genesis Utility Database • Recruitment Enrollment App • CensiTrac InstrumenTrac • Coaching into Care • Cochlear Custom Sound • **DSS DocManager** • IntelliWare TempTrak • Labtrac, Logicare • Lynx Duress Alarm Sys. • **MIRB 2002** • Noah Audiology Software • Nuance Output Manager • VistA Chemo Manager •	***Yes***	***Yes***	***Yes***	Social Security Number, EKG reading, Blood Pressure Name, Address, Medical treatment, and diagnosis documentation Research	This data is needed to facilitate patient care Also, data in this server is collected for VA Research Studies	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	Philadelphia VA Medical Center/ CMCVAMC
Server 2: • Candidate Stage Database • **iMed37-** MedConsent • iMedAudit iMed- Update	***Yes***	***Yes***	***Yes***	Social Security Number, Name, Address, Medical treatment, and diagnosis documentation	. This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	Philadelphia VA Medical Center /CMCVAMC

Server 3: • ANSOS PROD • ANSOSTEST • ARMESDVET • BESTVET • BESTVETFIDE • BESTVETTRK • BHL_PHI_Prod • BHL_PHI_Test • BHL_PrimeCare_Prod • **CEDCSE** • **CEDCSECM** • Cherp • CoachingIntoCareProd • CoachingIntoCare_Test • **COGPTSD** • **COGPTSDLOAD** • DATAENTRY • distribution • **DLM** • **Device Registration Service** • Streem FaxQueue2k • FORMSLIBRARY • **OM40SP2** • **ONDANS** • pckits • PHI_Biopoint_PI6 • PHICCDB • PHICCDBaudit • **PTSDBT** • **PTSDPUPIL** • **PTSDTHRP** • **QCDAO** • **REDLBID** • **ReportServerCoachCare** • **ReportServerCoachCareTempDB** • **RISKDRNK** • **SFFX** • **SystemState** • **teststudy** • **TOPG** • **TOPGMEDQ** • **TOPGSUB** • **TRACKING**	***Yes***	***Yes***	***Yes***	Social Security Number, Name, Address, Medical treatment, and diagnosis documentation Research	This data is needed to facilitate patient care Also, data in this server is collected for VA Research Studies	AES256 Encryption	Philadelphia VA Medical Center /CMCVAMC

• **TTAUDAA** • **TTAUDMEDQ** • Streem WorkflowLog2k Xerox Device Manager6							
Server 4: • PHLADELPHIPA DERM	***Yes***	***Yes***	***Yes***	Dermatology Medical Information Social Security Number, Name, Address, Medical treatment, and diagnosis documentation	This data is needed to facilitate patient care	AES256 Encryption	Philadelphia VA Medical Center /CMCVAMC
Server 5. **SQL_Test12**	***Yes***	***Yes***	***Yes***	Name, DOB, SSN	For testing VICTARS enhancements and corrections in a test environment	AES256 Encryption	VBA Insurance Center
Server 6: **SQL_PROD**	***Yes***	***Yes***	***Yes***	Name, DOB, SSN	Processing Veterans' Life Insurance Claims	AES256 Encryption	VBA Insurance Center