Date PIA submitted for review:

August 30, 2021

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

Area Alexandria

Continental District

Facilities Supported by the Area

Facilities Supported by the Area:
1. Alexandria VA Healthcare System
2. Natchitoches CBOC

[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.

3. Fort Polk Intake Center
4. Fort Polk CBOC
5. Lake Charles CBOC
6. Jennings CBOC
7. Lafayette Campus A CBOC
8. Lafayette Campus B CBOC
9. Rapides Parish Vet Center

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): Sandra Shirah	318-483-5018	Sandra.shirah@va.gov	Alexandria VA HCS

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): Albert Comple	318-466-2080	albert.comple@va.gov	Alexandria VAMC

Name	Phone Number	Email Address	Location
Yentl Brooks	713-383-1879	Yentl.brooks@va.gov	Michael DeBakey Medical Center, Houston, TX

Area Manager

Name	Phone Number	Email Address	Location
Obie Ward	318-466-2294	Obie.ward@va.gov	Alexandria VA HCS

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 Alexandria is an Information Area Boundary that consists of Alexandria VA HCS, Natchitoches, Fort Polk, Bayne-Jones Army Hospital, Lake Charles, Jennings, Lafayette Campus A, Lafayette Campus B, and Rapides Vet Center. The Area Boundary environment consists of components such as workstations, laptops, portable computing devices, terminals, servers, printers, and IT enabled networked medical devices that are owned, managed, and maintained by the facilities. The Area provides operational connectivity services necessary to enable users' access to information technology resources throughout the enterprise including those within the facility, between facilities, resources hosted at data centers, and connectivity to other systems. Network connectivity rules are enforced by VA approved baselines for router and switch configurations. The Area Boundary system environment also includes as applicable, subsystem storage utilities such as tape drives, optical drives, disk drives, network area storage (NAS), storage access networks (SAN), archival appliances, special purpose systems, and tier 2 storage solutions. The Area Boundary encompasses the management, operational, and technical security controls associated with IT hardware, consisting of servers, routers, switches, hubs, gateways, peripheral devices, desktop/laptops, and OS software. The Area Boundary employs a myriad of routers and switches that connect to the VA network.

Overview

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

- *The IT Area Boundary name and the name of the sites within it.*
- *The business purpose of the Area Boundary and how it relates to the program office and agency mission.*

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

The Alexandria VA Health Care System is a facility level system that operates under the authority of **Veterans' Benefits**, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and **Veterans Health Administration – Organization and Functions**, Title 38, U.S.C., Chapter 73, §7301(a). The system includes servers, workstations, laptops, printers and commercial-off-the-shelf applications). It supports mission-critical and other systems necessary to conduct day-to-day operations by providing access to electronic resources.
The system contains and transmits contact, personal health, military, and financial information on veterans, their dependents, volunteers, employees, and contractors. The system is a new system that was created mid-year 2013, when the Office of Information and Technology made major changes to VA systems and their security boundaries. Consequently, Personally Identifiable Information (PII) and Sensitive Personal Information (SPI) now reside on this system. This data ownership remains at the facility level and many of the decisions related to the collection, use, storage, and dissemination of the data are made at the facility level. Approximately 41,384 individual's PII and SPI is stored. This figure includes employees, inpatient and outpatients in priority groups 1-8, at the main facility in Alexandria as well as the Community Based Outpatient Clinics (Leesville, Lafayette, Lake Charles, Natchitoches and Jennings).

The Alexandria VA Health Care System is an interconnected information resource under the same direct management control that shares common functionality. It includes local area network hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. The system is continuously used during business and non-business hours, supporting business processes related to the VA and its computing environment. The confidentiality, integrity and availability of the system is critical, i.e., ensuring that data is only received by the persons and applications that it is indented for, that data is not subject to unauthorized or accidental alterations, and that the resources are available when needed. Due to the sensitivity of the interconnected information resources of the system, all VA personnel with network/system access are required to have some type of a background investigation to fulfill their duties.

Internal sharing, discussed in greater detail in Section 4 of this Privacy Impact Assessment (PIA), is generally done to ensure that veterans and their families receive the benefits and care that they have earned. Alexandria VA Health Care System shares patient data with VA General Counsel, VHA programs or contractors with a business need to know, Veteran Benefits Administration, National Veteran Service Organizations, National Cemetery Administration, VA Network Authorization Office-Non VA Care, VA Veteran Centers, Health Eligibility Center and Austin Automation Center. External sharing is discussed in greater detail in Section 5 of this PIA.

The following VA System of Record Notices (SORNs) apply to the General Support System:
:
• *Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attending's, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records-VA,* SORN 14VA05135
• *Non-VA Fee Basis Records*-VA, SORN 23VA163
• *Patient Medical Records*-VA, SORN 24VA19
• *Veteran, Patient, Employee, and Volunteer Research and Development Project Records*- VA, SORN 34VA12
• *Community Placement Program*-VA, SORN 65VA122
• *Health Care Provider Credentialing and Privileging Records*-VA¸SORN 77VA10Q
• *Veterans Health Information Systems and Technology Architecture (VistA) Records*-VA, SORN 79VA10P2
• *Income Verification Records*-VA, SORN 89VA19
• *Automated Safety Incident Surveillance and Tracking System*-VA, SORN 99VA131
• *Telephone Service for Clinical Care Records*- VA, SORN 113VA112
• *The Revenue Program Billings and Collection Records*-VA, SORN 114VA16
• *National Patient Databases*-VA, SORN 121VA19

Each VA facility has a system, supporting mission-critical and other systems necessary to conduct day-to-day operations within the Veterans Health Administration. Applications and devices within the system support numerous areas, including VistA, Vista Imaging, VistA RO, user file storage, backups, and other non-VistA applications.

Veteran, veteran's primary contact and volunteer's service, medical, criminal record, guardian, education and benefit information may be collected as well as contractor and employee personnel and payroll records may be collected, processed and retained.

The information is collected and used for the medical and mental health treatment of eligible individuals. Additional information is maintained regarding employees based on HR and payroll needs.
The District 4, Territory 2 system accreditation boundary consists of facilities located within five Veterans Integrated Service Networks (VISNs) in the central United States and support communications to extended LAN locations such as community-based outpatient clinics (CBOC's).

The system is comprised of workstations, terminals, servers, printers, and other devices that support communications. The system includes magnetic tape drives, Optical drives, disk drives, and uninterruptible power supplies (UPS). The system also includes network area storage (NAS), storage access networks (SAN), jukeboxes, Archive Appliances, and NetApp Tier 2 storage solutions.

Access to the system is via wired or wireless devices using TCP/IP and other protocols operating on a variety of operating systems as approved by VA Baselines. Devices which comprise the system include government furnished equipment (GFE) such as: personal computers, thin clients, portable computing devices and medical device systems.

Access to configure system devices is controlled through authentication servers using Active Directory. Access to the system is via workstations operating on VA approved baselines throughout the Medical Centers, CBOCs, Vet Centers and the Local Area Networks of its affiliates. Microsoft Windows client workstations connect over a Windows network and may use terminal emulation software and the Remote Procedure Call (RPC) Broker to connect to other systems, such as VistA. Clients primarily connect over

the TCP/IP network using terminal emulation software and remote procedure call (RPC) broker to VistA or other network resources such as file, print or application servers and telephone systems.

Vista Imaging is a multi-media online patient record to integrate traditional medical chart information with medical images of all kinds including x-rays, pathology slides, video views, scanned documents, cardiology exam results, wound photos, dental images, endoscopies, etc. Images can be acquired using clinical workstations or with automatic Digital Imaging and Communications in Medicine (DICOM) standard interfaces. The Veterans Health Administration has developed a communications infrastructure to support access to medical data, including images and text report data, between Veterans Health Administration medical centers nationwide. This allows clinicians to view appropriate patient data located at remote sites from virtually any location. Vista Imaging is the VA system of Record for all patient multimedia data.
Access to external resources outside the LAN boundary will conform to national wide area network (WAN) guidelines on configuration and usage. WAN security is outside facility control and beyond the scope of this document. There is access from the Intranet to both the VA's wide area network (WAN) and to the Internet via the VA Internet Gateways. VA-approved firewalls are positioned between the Intranet and the Internet Gateways.

Area Alexandria does collect, use, disseminate, maintain, and store PII/PHI.
The VHA facility located within the Area Alexandria IT Boundary accesses VA Enterprise IT systems respectively, hosted and maintained outside of this boundary. These are VISTA, VBMS, etc.

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

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, etc. There are individual PIAs that contain detailed information on the maintenance, dissemination and sharing practices, and storage of the PII/PHI for each Enterprise system accessed by the facilities.

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

The applicable SORs for Area Alexandria include:

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	***Applicable SORs*** ****Please verify that the below SORs are applicable to your Area. Please add any additional applicable SORs to the table and remove those that are not applicable.***
VHA	• Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attendings, and Other or Paid Indirectly through a Disbursement Agreement) Personnel Records-VA, SORN 14VA05135 • 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

Site Type: VBA/VHA/NCA or Program Office	*Applicable SORs* ***Please verify that the below SORs are applicable to your Area. Please add any additional applicable SORs to the table and remove those that are not applicable.***
	• Health Care Provider Credentialing and Privileging Records-VA ,SOR 77VA10E2E • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10 • Income Verification Records-VA, SOR 89VA10NB • Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA13 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10 • National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147VA10NF1 • VHA Corporate Data Warehouse- VA 172VA10A7 • Health Information Exchange - VA 168VA005

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)

PII Mapping of Components

Area Alexandria consists of **8** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected within Area Alexandria 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 on the system or is collected or maintained and/or disseminated by the Area Alexandria 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 programs and resources in the Veterans Benefits Administration (VBA), the VA Health Eligibility Center (HEC), VA Network Authorization Office (NAO) for non-VA Care payments, and non-VA medical providers. In the case of a Veteran with a disability directly connected to their military service, the VBA may also provide service-connected disability ratings and information related to applicable disabilities (date granted, type of disability, overall percentage of combined disabilities).

The information collected, maintained and/or disseminated by ALX-VHA SYSTEM comes from a variety of resources. The largest amount of data comes directly from individuals and is also collected from
data already provided to other organizations within the VA, including:

- Austin Automation Center (AAC)
- Veteran's Health Administration programs
- Veterans Benefits Administration (NOLA Regional Office)

Additional data come from external Federal Agencies. These agencies include:

• Office of Personnel Management (OPM) to determine military service and employment eligibility, results of employment background investigations.
• Federal Emergency Management Agency (FEMA)
• Social Security Administration (SSA) to determine eligibility for Federal benefits

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
- Office of Personnel Management (OPM) to determine military service and employment eligibility, results of employment background investigations.
- Federal Emergency Management Agency (FEMA)
- Social Security Administration (SSA) to determine eligibility for Federal benefits

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.

Information is collected from individuals verbally via interviews and conversations with VA medical and administrative staff, in writing (such as on VA Form 10-5345, *Request For and Authorization To Release Medical Records Fillable*), and via electronic and web form submissions.

Information is also collected from a variety of other IT systems and resources internal and external to the VA. These data collections may be done using secure web portals, Virtual Private Network (VPN) connection, Health Level Seven (HL7) links, VA/Department of Defense (DOD) gateway, Hospital Inquiry HINQ, and Commercial off-the-shelf (COTs) application, Decision Support System (DSS), Fee Basis Claims (FBCS) systems.

Means of Collection Table

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

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

Information from outside resources comes to the Area Alexandria using several methods. Chief among these sources, are the DoD, SSA, and IRS. The DoD provides military records, including medical records compiled when the patient was a member of the US Military. Income information is verified using information from the Social Security Administration (SSA) and the Internal Revenue Service (IRS).

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

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

Include a statement of why the particular PII/PHI is collected, maintained, used, or disseminated in the Area Boundary is necessary to the program's or agency's mission. Merely stating the general purpose of the Area Boundary without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the Area Boundary collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the Area Boundary's purpose.

This question is related to privacy control AP-2, Purpose Specification.

The purposes of the information from Veterans and other members of the public collected, maintained, and processed by Area Alexandria 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 analysis of data.
Purposes include:
1.To determine eligibility for health care and continuity of care
2.Emergency contact information is cases of emergency situations such as medical emergencies
3.Provide medical care
4.Communication with Veterans/patients and their families/emergency contacts
5.Determine legal authority for providers and health care workers to practice medicine and/or subject matter expertise
6.Responding to release of information request
7.Third party health care plan billing, e.g. private insurance
8.Statistical analysis of patient treatment
9. Contact for employment eligibility/verification
Employee and VA contractor information is maintained based on Human Resources (HR) and payroll needs and Federal contracting requirements.

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

Site Type: VBA/VHA/NCA or Program Office	*Purpose of Information Collection*
	• Statistical analysis of patient treatment • Contact for employment eligibility/verification

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

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

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

Information obtained directly from the individual will be assumed to be accurate. Information may be verified with other Federal agencies (VBA, DOD, SSA and IRS) to confirm eligibility or benefits. Should conflicting information come to the attention of facility staff, it will be documented and verified prior to further use.
Furthermore, individuals have the right to obtain access to their records and request correction to them when necessary. Patient demographic as well as income verification matching completed by automated tools with connections to the Austin Automation Center (AAC) are obtained. Practitioners review and sign all treatment information and Health Information Management Service reviews data obtained and assists with corrections.
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.
Information that is collected and used directly from enterprise systems have additional details regarding checks for accuracy in their own enterprise level PIAs.

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

Information is checked through the VBA to verify eligibility for VA benefits. Information about military service history is verified against official DoD military records and income information is

verified using information from the Social Security Administration (SSA) and the Internal Revenue Service (IRS).

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

The Area Alexandria is a facility level entity that operates under the authority of **Veterans Health Administration – Organization and Functions**, Title 38, U.S.C., Chapter 73, § 7301(a)

Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:
• **Health Insurance Portability and Accountability Act of 1996** (**HIPAA**), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).
• **Health Information Technology for Economic and Clinical Health (HITECH) Act,** Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), *codified at* 42 U.S.C. §§300jj *et seq.*; §§17901 *et seq.*
• **Privacy Act of 1974**, 5 U.S.C. 552a
• **Federal Information Processing Standards (FIPS) 140-2,** approved encryption algorithms and products
• **Federal Information Processing Standards Publication (FIPS PUB) 199**, Standards for Security Categorization of Federal Information and Information Systems
• **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47,** Security Guide for Interconnecting
• **National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 60,** Guide for Mapping Types of Information and Information Systems to Security Categories.
• **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53**, Rev. 4, Recommended Security Controls for Federal Information Systems
• **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88**, Guidelines for Media Sanitization
• **Alexandria VA Health Care System local MCP 00PO.01,** Privacy Policy.
• **Trade Secrets Act** (18 U.S. Code 1905)
• **Unauthorized Access Act** (18 U.S. Code 2701 and 2710)
• **VA Directive 6371**, Destruction of Temporary Paper Records
• **VA Directive 6600,** Responsibility of Employees and Others Supporting VA in Protecting Personally Identifiable Information (PII)
• **VA Directive and Handbook 6500,** Information Security Program
• **VA Directive and Handbook 0710,** Personnel Suitability and Security Program

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.

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: Area Alexandria contains sensitive personal information – including social security numbers, names, dates of birth and protected health information – on veterans, members of the public, & VA employees and contractors. 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 harm or even identity theft may result.

Mitigation: Veterans Health Administration (VHA), Continental District as well as the Alexandria Veterans Health Care System deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors within the region. The security measures include access control, configuration

management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation.

Section 2. Uses of the Information

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

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

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

Patient and employee data are analyzed on an as-needed basis with tools such as Decision Support System (DSS)/ Release of Information (ROI), Bed Management System (BMS), Auto Compliance Management (ACM), Prosthetics GUI, and Coding Compliancy Module (CCM) upon official authorization. Alexandria Veterans Health Care System uses statistics and analysis to create various reports which provide a better understanding of patient care and employee needs.

These reports may track:

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

2.3 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> 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.

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

Area Alexandria follows national VA policies regarding information retention. The records include information concerning current and former employees, applicants for employment, trainees, contractors, sub-contractors, contract personnel, students, providers and consultants, patients and members of their immediate family, volunteers, maintenance personnel, as well as individuals working collaboratively with VA.

- 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 of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your Area 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.

When managing and maintaining VA data and records, Area Alexandria will follow the guidelines established in VA Record Control Schedule (RCS)-10 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf) as well as RCS 005-1 (http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf).
These documents specify how long records will be retained by the VA, if/when they will be transferred to a national records storage location, and the length of time the records will be stored at the national level. For greater details related to records retention at the Veterans' Health Administration, please review RCS-10 and RCS-005-1.

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.

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.

When managing and maintaining VA data and records, Area Alexandria follows the guidelines established in the NARA-approved **Department of Veterans' Affairs Record Control Schedule (RCS)-10** (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf); **Department of Veterans Affairs, Office of Information & Technology RCS 005-1**(http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf) and the **General Records Schedule** (http://www.archives.gov/records-mgmt/grs/).
Version *Retention Schedule Table*

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

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

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

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

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8310
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 Handbook 6500.1, Electronic Media Sanitization** (November 3, 2008), http://www.va.gov/vapubs/ viewPublication.asp?Pub_ID=416&FType=2.
When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1.
Digital media is shredded or sent out for destruction per VA Handbook 6500.1.
Additionally, ALXVAHCS follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents **as well as** FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

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

Area Alexandria does not have a research program.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>
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.

Follow the format below:
Privacy Risk: There is a risk that the information maintained by Area Alexandria 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 or breached or exploited for reasons other than what is described in the privacy documentation associated with the inform

Mitigation: In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed in the system is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary. To mitigate the risk posed by information retention, Alexandria VA Health Care System 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 Alexandria VA Health Care System 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 facility 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 inform

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

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

Note: Question #3.6 (second table) in the Area Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT Area 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 Officeor IT System information is shared/received with	***List the purpose of theinformation being shared /received with the specified program office or IT system***	***List the specific data element types such as PII/PHI that are shared/received with the Program Office or ITsystem***	***Describe the method oftransmittal***
Department of Veterans Affairs General Counsel Office	Assistance in investigation of patient oremployee claims.	Pertinent PII, PHI, and Individually Identifiable Information (III) appropriate to the request.	Transmitted upon requestin an electronic, written or verbal format based onthe individual request.
VHA programs or contractors with a business need to know	Access for assistancewith the Wounded Warrior Project	Pertinent PII, PHI, and IIIappropriate to the request	Transmitted upon requestin an electronic, written or verbal format based onthe individual request.
Veterans Benefits Administration	Examinations and eligibility for VAbenefits.	Pertinent PII, PHI, and IIIappropriate to the request.	Transmitted electronically for purposes of Compensation and Pension ratings.

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

National Veteran's Service Organizations – specific organization suchas Veterans of Foreign War (VFW), etc.	The organization helps members apply for VAbenefits	Pertinent PII, PHI, and IIIappropriate to the request	Transmitted upon requestin an electronic, written or verbal format based onthe individual request.
National Cemetery Administration	Verification of deathbenefits.	Pertinent PII, PHI, and IIIappropriate to the request.	Transmitted upon requestin an electronic, written or verbal format based onthe individual request.
VA Network Authorization Office-Non-VA Care	Health/medical payment authorization	Demographics, diagnoses,medical history, service connection, provider orders, VHA recommendation/appr ovalfor non-VA care	Fee Basis Claim System(FBCS) authorization software program
VA Veteran Centers	Continuity of care, eligibility, and enrollment	Access to health information for plan of treatment	Electronically viewed through the Computerized Patient Record System (CPRS)
Health Eligibility Center(HEC)	Healthcare eligibility information	Name, Date of Birth, Sex,SSN, demographics and health information	Information may be transmitted electronically.
Austin Automation Center (AAC)	Healthcare encounter information	Name, Date of Birth, Sex,SSN, demographics and health information	Information may be transmitted electronically. AAC employees can log intoCPRS or VistA

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The sharing of data is necessary for the medical care of individuals eligible to receive care at the Alexandria VAHCS. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation.

Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

The use of a Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two-factor authentication.

Microsoft Outlook is also another tool that is used to share internal information within the organization. Risks are mitigated by using encryption methods to share sensitive information within the organization.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the facility is allowed to share the information in identifiable form or personally identifiable information outside of VA.

Note: Question #3.7 in the Area Privacy Threshold Analysis should be used to answer this question.

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

For each interface with 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

Common external state organizations may include: State Adult Protective Services, State Department of Health/Public Health, State Officer of Children and Family Services, or State University Hospitals and Clinics.

Common external private organizations may include: Administrative and Technological Support Organizations, Document Shredding/Destruction Organizations, Healthcare Providers, Insurance Providers, Medical Diagnostic Organizations, or Privacy University Hospitals and Clinics].

Data Shared with External Organizations

List External Program Office orIT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office orIT system***	***List the specific data element typessuch as PII/PHI that are shared/received with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can bemore than one)***	***List the method of transmission and themeasures in place tosecure data***
ALERE	Remote Support – Diagnostic ITTools	System Log files, sample clinical data that may contain Protected Health Information (PHI) appropriateto the agreements	Nationa l ISA/M OU	Site to Site VPN

Data Shared with External Organizations

Department of Defense (DOD)	Determine militaryservice dates, Eligibility	Name, Date of Birth, Sex, SSN, demographics andhealth information	SORN 24VA10 P2, Routine use 1, National sharing agreement, VA SORN 168VA1 0P2	Information is uploaded/download edelectronically to the database.
Draeger ~ INNOVIAN	Remote Support – Diagnostic IT Tools	System Log files, sample clinical data that may contain Protected Health Information (PHI) appropriateto the agreements	National ISA/MO U and BAA	S2S VPN
VHA Freedom of Information Office ~ FOIAEXPRESS	Legal/regulatory	Pertinent PII, andIII appropriate to the request including but notlimited to name, demographics, as it relates to any VA record.	Legal authority and binding agreemen t	Information is uploaded electronically to the database.
GE MED-IT ~ MUSE	Remote Support –Diagnostic IT Tools	System Log files, sample clinical data that may contain Protected Health Information (PHI) appropriateto the agreements	National ISA/MO U	Site to Site VPN

Data Shared with External Organizations

LABCORP	Remote Support –Diagnostic IT Tools	System Log files, (no PII/PHI data is transmitted electronically, onlyhardcopy).	National ISA/MOU	Site to Site VPN FOR TECH SUPPORT ONLY
Philips Healthcare	Remote Support –Diagnostic IT Tools	System Log files, sample clinical data that may contain Protected Health Information (PHI) appropriateto the agreements	National ISA/MOU	Site to Site VPN
Office of Personnel Management (OPM)	Determine military and civilian service dates, employment eligibility	Pertinent Personally Identifiable Information (PII) and Individually Identifiable Information (III). Name, DOB, demographics, SSN, all employee HR records.	National ISA/MOU	Information is uploaded/downloaded to/from electronic database.

Data Shared with External Organizations

Federal Emergency Management Agency (FEMA)	Eligibility for Federal benefits	First and last name, SSN, dob	Homeland Security Presidential Directive – 5 requires all federal agencies to comply as required with FEMA directives during emergencies.	Inquiries will normally come through the VHA Office of Emergency Management with coordination through the VISN EM and executive leadership. In the rare case that data is requested directly, the data would be provided via encrypted email, ensuring that executive leadership, the VISN and OEM are included in the response. Information may be transmitted upon request in an electronic, written or verbal format.
Social Security Administration (SSA)	Eligibility for Federal benefits	Name, Date of Birth, Sex, SSN, demographics and health information	Title 38, United States Code, Section 5701 National ISA/MOU	Documents faxed to agency weekly, or more often as requested.
TriWest HealthCare Alliance (TRIWEST)	Community Care National Program	Service dates, SSN, demographics, service connection; clinical packet (from CPRS).	National ISA/MOU	Scanned documents uploaded into shared software program
Vecna Robotics (VECNA)	Remote Support – Diagnostic IT Tools	System Log files, sample clinical data that may contain Protected Health Information (PHI) appropriate to the agreements	National ISA/MOU	Site to Site VPN

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

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

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

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

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

Follow the format below:

Privacy Risk: The sharing of data is necessary for the medical care of individuals eligible to receive care at Alexandria VAHCS. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation.

All personnel accessing Veteran's information must first have a successfully adjudicated background screening (SAC). This background check is conducted by the Federal Bureau of Investigation (FBI)

Justice Information and criminal history records. A background investigation is required commensurate with the individual's duties.

Individual users are only given job position specific access to individually identifying data through the issuance of a user ID and password.

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 Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A signed statement acknowledging that the individual read and understood the NOPP is scanned into each applicant's electronic file. When updates are made to the NOPP copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.
The Department of Veterans Affairs provides additional notice of this system by publishing 2 System of Record Notices (SORNs):

1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Feb. 11, 2014), in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2014-08-14/pdf/2014-19283.pdf

2) The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10P2 (Amended Oct. 31, 2012), in the Federal Register and

online. An online copy of the SORN can be found at:
https://www.oprm.va.gov/docs/sorn/SORN79VA10P2.PDF

The following VA System of Record Notices (SORNs) apply to the System:
• *Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attending's, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records-VA,* SORN 14VA05135
• *Non-VA Fee Basis Records*-VA, SORN 23VA163
• *Patient Medical Records*-VA, SORN 24VA19
• *Veteran, Patient, Employee, and Volunteer Research and Development Project Records*- VA, SORN 34VA12
• *Community Placement Program*-VA, SORN 65VA122
• *Health Care Provider Credentialing and Privileging Records*-VA,SORN 77VA10Q
• *Veterans Health Information Systems and Technology Architecture (VistA) Records*-VA, SORN 79VA10P2
• *Income Verification Records*-VA, SORN 89VA19
• *Automated Safety Incident Surveillance and Tracking System*-VA, SORN 99VA131
• *Telephone Service for Clinical Care Records*- VA, SORN 113VA112
• *The Revenue Program Billings and Collection Records*-VA, SORN 114VA16
• *National Patient Databases*-VA, SORN 121VA19
• https://www.oprm.va.gov/privacy/systems_of_records.aspx

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 Veterans' Health Administration (VHA) as well as Area Alexandria only requests information necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this will prevent them from obtaining the benefits necessary to them. Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with Area Alexandria.

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

Yes, individuals may request in writing a record restriction limiting the use of their information by filling out a 10-5345 form. 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 Release of Information 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, guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information.

VHA permits individuals to give consent or agree to the collection or use of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. If individuals are not willing to give information verbally then they are not required to do so. Individuals are made aware of when they must give consent when there is data collected about them through the VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by VHA Central Office periodically to ensure compliance with various requirements including that Privacy Act Statements which are on forms that collect personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations where required. If the individual does not want to give consent then they are not required to in most cases unless there is a statute or regulation that requests the collecting and then consent is not necessary but when legally required VHA obtains a specifically signed written authorization for each intended purpose from individuals prior to releasing, disclosing or sharing PII and PHI.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:
Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and Area Alexandria prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries and periodic monitoring is performed to check that the signed acknowledgment form has been scanned into electronic records. 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 (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

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.

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 myHealthevet program, VA's online personal health record. More information about myHealthevet is available at https://www.myhealth.va.gov/index.html.

In addition to the procedures discussed above, the SORNs listed in the Overview section of this PIA each address record access, redress, and correction. Links to all VA SORNs can be found at https://www.oprm.va.gov/privacy/systems_of_records.aspx

Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative to obtain information upon request.

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.

Request must be in writing and specify why the individual believes the information to be inaccurate, incomplete, irrelevant, and/or untimely and the reason for this belief. Use of the optional "Amendment Request Form," available through Privacy Office, Release of Information and Patient Advocate Officers, is encouraged. The request must be adequately describing the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief.

Once completed form is received by Privacy Officer, the writer of the inaccurate/erroneous note will be consulted regarding the amendment. Should request be denied at writer's level, Veteran's request is elevated to the Service Chief, and then to Chief of Staff, who has final authority. Should the request be approved at any level, Privacy Officer will make authorized corrections and notify Veteran within 30 calendar days. Veteran will receive written notification of any delay during the process. Point of Contact for amendments is the Privacy Officer.

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

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

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

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

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

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

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

Information can also be obtained by contacting the Area Alexandria ROI or Privacy Office.

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

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

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Veterans and other individuals are encouraged to use the formal redress procedures discussed above in Section 7.3 to request edits to their personal medical records and other personal records retained about them.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Privacy Risk: There is a risk that a Veteran may not know how to obtain access to their records or how to request corrections to their records.

Mitigation:
Upon receiving a copy of the Notice of Privacy Practices (NOPP), which every patient treated as a Humanitarian Emergency receives, it explains the process of amending the medical record. Beneficiaries (Veterans) are reminded of this information with the NOPP is mailed annually to them by the VA Privacy Office.

The Area Alexandria Release of Information (ROI) office is available to assist Veterans with obtaining access to their medical records and other records containing personal information.

The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll to obtain access to all the available features.

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.

Access to Area Alexandria's working and storage areas is restricted to VA employees who must complete both the HIPAA and Information Security training. Specified access is granted based on the employee's functional category. Role-based training is required for individuals with significant information security responsibilities to include but not limited to Information System Security Officer (ISSO), local Area Manager (AM), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

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

Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.

Access to computer rooms at the Alexandria VAHCS facilities is limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Information that is downloaded from VistA and maintained on laptops and other approved government equipment is afforded similar storage and access protections as the data that is maintained in the original files. 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 Area Alexandria or an OIG office location remote from the hospital, is controlled in the same manner.

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.

Each contract is reviewed prior to approval based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee). This review is conducted each time the contract period expires.
Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, signing the contractor Rules of Behavior, VHA HIPAA training as well as the appropriate background investigation to include fingerprinting. Certification that these items have all been completed by all contractors must be provided to the VHA 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

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 training. In addition, all employees who interact with patient sensitive medical information must complete the VA mandated privacy HIPAA training. Finally, all new employees receive face-to-face training by the Area Alexandria Privacy Officer and Information System Security Officer during new employee orientation. The Privacy and Information System Security Officer also perform subject specific trainings on an as needed basis.

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

If Yes, provide:

1. *The Security Plan Status, Approved*
2. *The Security Plan Status Date, 06/25/2021*
3. *The Authorization Status, Authorized – 1 year ATO*
4. *The Authorization Date, 10/02/2020*

5. *The Authorization Termination Date, 10/02/2021*
6. *The Risk Review Completion Date, 09/16/2020*
7. *The FIPS 199 classification of the system is MODERATE*

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

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**

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

Signature of Privacy Officers

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

Sandra K Shirah 218686 Digitally signed by Sandra K Shirah 218686
Date: 2021.10.20 11:37:22 -05'00'

Privacy Officer, Sandra Shirah

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.

Digitally signed by Albert P. Comple 912479

Information Systems Security Officer, Albert Comple

YENTL BROOKS

Digitally signed by YENTL BROOKS
Date: 2021.10.25 11:26:15 -05'00'

Information Systems Security Officer,Yentl Brooks

Signature of Area Manager

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

Obie E. Ward Digitally signed by Obie E. Ward 155919 Date: 2021.10.20 07:53:15 -05'00'

Area Manager, Obie Ward

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:**

APPENDIX B – PII Mapped to Components

The completion of this section of the PIA will be in coordination with the Area Manager, Privacy Officer and ISSO. They may need to coordinate with the system (server/database) point of contact. This information must match the servers/databases listed in 3.6 of the Area PTA.

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

PII Mapped to Components Table

Components of the Area Boundary collecting/storing PII *(Each row refers to a grouping of databases associated with a single server)*	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Provide Names of Applicable Sites***
• **NOAHDatabaseCore**	Yes	Yes	Yes	Name, Last 4 of SSN, DOB	This data is needed to facilitate patient care for audiology (hearing aids)	Server is stored in a secured environment and managed with restricted access controls	Alexandria VAHCS