Date PIA submitted for review:

Aug 9, 2023

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

Area Tuscaloosa Southeast District Area Boundary

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

Sites within Boundary:

Sites	***Station Numbers***
1) Tuscaloosa VAMC	679
2) Selma CBOC	679
3) Fayette Store	679
4) Hamilton Storefront	679
5) Demopolis Storefront	679
6) University of Alabama Vet Clinic	679

Boundary Contacts:

Boundary Key Stakeholders

Name	***Title (PO, ISSO, AM, MD/SPS Staff, Facility Director)***	***Phone Number***	***Email Address***	***Applicable Site (VBA, VHA, NCA, Program Office)***
Michael Culver	Privacy Officer	205-554-2885	Michael.Culver2@va.gov	**VHA**
Shionell Williams	Information System Security Officer (ISSO)	205-957-3882	Shionell.Williams@va.gov	**VHA**
Bryant Lewis	Area Manager	205-554-3660	Bryant.Lewis@va.gov	**VHA**

Abstract

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

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

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *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*

- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*

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

The Department of Veterans Affairs uses the Veterans Health Information Systems and Technology Architecture, better known as VistA, an Electronic Health Record (EHR) system that provides an integrated inpatient and outpatient electronic health record for VA patients, and administrative tools to help VA deliver the best quality medical care to Veterans. VistA is used in all Veteran's Health Administration (VHA) hospitals, medical centers, and outpatient clinics, forming an interconnected EHR that makes a veteran's VAmedical record accessible throughout the main VHA facility and connected clinics where the EHR is maintained.

The VistA system is a customizable system that allows each VA facility and medical center to choose to install minor applications or programs on the facility's instance of VistA. These minor applications can include clinical applications such as Immunology Case Registry (ICR) and the VistA Imaging System; administrative applications such as Veteran Income Match Verification and Volunteer Timekeeping; and VistA infrastructure applications such as the Master Patient Index and the Patient Data Exchange. These toolsand many others, allow each facility to customize how it employs the VistA system.

The Tuscaloosa VA Medical Center Vista System 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 VistA (e.g., All facility VistA systems will be rolled up into one Regional VistA boundary consisting of VistA's Massachusetts General Hospital Utility Multi- Programming System, later changed to Multi-User Multi-Programming System (MUMPS) environment; its applications, users stored in "dat" files) to support mission-critical and other systems necessary to conduct day-to-day operations within the Veterans Health Administration by providing access to electronic resources. The Tuscaloosa VA Medical Center VistA collects, processes, and/or retains the information of over one million veterans, contractors and VA employee information, and encompasses the facility level VistA of the following Veteran's Health Systems:

TUA-VHA Tuscaloosa VA Medical Center

The Tuscaloosa VA Medical Center VistA information system boundary does provide security oversight and a variety of support functions to the facilities and their local VistA Systems, 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. For example, the Tuscaloosa VA Medical Center staff will independently decide whether or not to share data with state level veterans' assistance organizations.

The Tuscaloosa VA Medical Center VistA utilizes the VistA system to collect data already provided to otherorganizations within the VA, including at a minimum with the Veteran's Benefit Administration (VBA) and the Austin Acquisition Center (AAC). Additional data, such as confirmation of military service or results of employee background checks, come from external Federal Agencies. These agencies include at a minimum: Department of Defense (DOD), Internal Revenue Service (IRS), Office of Personnel Management (OPM), Social Security Administration (SSA), Federal Emergency Management Agency (FEMA) as well as the Federal Bureau of Investigation (FBI).

The Tuscaloosa VA VistA serves Veterans through its access and control of all IT functions in each facilityutilizing the VistA software programs. The information is used to conduct healthcare, compensation and pension, income verification, patient eligibility, insurance information, employee/contractor information.

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

The application SORs for Tuscaloosa includes:

Site Type: VBA/VHA/NCA or Program Office	***Applicable System of Records (SORs)***
VHA	• Non-VA Fee Basis Records-VA, SOR 23VA10NB3 • Patient Medical Records-VA, SOR 24VA10A7 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA10 • Community Placement Program-VA, SOR 65VA122 • Health Care Provider Credentialing and Privileging Records-VA¸SOR 77VA10E2E • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10 • Income Verification Records-VA, SOR 89VA10NB • Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA13 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10 • National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147VA10NF1 • VHA Corporate Data Warehouse- VA 172VA10A7 • Health Information Exchange - VA 168VA005

Section 1. Characterization of the Information

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Account Information
☒ Health Insurance Beneficiary Numbers
☒ Account numbers
☒ Certificate/License numbers
☒ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Current Medications
☒ Previous Medical Records
☒ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☒ Next of Kin
☒ Guardian Information
☒ Electronic Protected Health Information (ePHI)
☒Military History/Service Connection
☒Service-connected Disabilities
☒Employment Information
☒ Veteran Dependent Information
☒ Disclosure Requestor Information
☒ Death Certification Information
☒ Criminal Background
☒ Education Information
☒ Gender
☒ Tumor PHI Statistics
☒ Other Unique Identifying Information (list below)

PII Mapping of Components (Servers/Database)

Area Tuscaloosa consists of 3 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 Tuscaloosa and the reasons for the collection of the PII are in the Mapping of Components Table in Appendix B of this PIA.

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

The Veterans Health Information Systems and Technology Architecture (VistA) consists of three (3) key components. The component has been analyzed to determine if any elements of that component collect PII. Thetype of PII collected by VistA and the functions that collect it are mapped below.

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

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

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

1.3 How is the information collected?

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

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

Information is collected directly from patients, employees and/or other members of the public is collected using paper forms (such as the VHA Form 10-10EZ enrollment form for VA health care which can be located at http://www.va.gov/vaforms/medical/pdf/vha-1010EZ-fill.pdf), or interviews and assessments with the individual. Information from outside resources comes in several ways. Among these sources, are the Department of Defense (DoD) and the Veterans Benefits Administration (VBA). The DoD provides military records, including medical records compiled when the patient was a member of the US Military. The VBA provides records which include the type and percentage of granted 'service-connected' disabilities, the dates of service-connected disability ratings, and, in some cases, the VBA populates patient demographics to the Tuscaloosa VA GSS in order for the Tuscaloosa VA to provide a Compensation and Pension examination to a claimant. These outside records are transmitted through a secure shared computer linkage.

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

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

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

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

Site Type: VBA/VHA/NCA or Program Office	***Purpose of Information Collection***
VHA	• To determine eligibility for health care and continuity of care • Emergency contact information is cases of emergency situations such as medical emergencies • Provide medical care • Communication with Veterans/patients and their families/emergency contacts • Determine legal authority for providers and health care workers to practice medicine and/or subject matter expertise • Responding to release of information request • Third party health care plan billing, e.g., private insurance • Statistical analysis of patient treatment • Contact for employment eligibility/verification

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

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

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

Information obtained directly from the individual will be assumed to be accurate. Furthermore, individuals have the right to obtain access to their records and request correction to them when necessary (see Section 7 for additional information). Patient demographic as well as income verification matching completed by automated tools with connections to the Austin Automation Center are obtained. Practitioners review and sign all treatment information and Business Office/Health Information Management Service reviews data obtained and assists with corrections.

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

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

List the full legal authority for operating the 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.

The Tuscaloosa VA Medical Center VistA System 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)
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.*

1.7 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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?*

Follow the format below when entering your risk assessment:

Privacy Risk:

Tuscaloosa VA Medical Center VistA contains sensitive personal information – including social security numbers, names, 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 could potentially occur.

Mitigation:

VA Tuscaloosa employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control, awareness and training, audit and accountability, certification, accreditation, and security assessments, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and system and information integrity. The area employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives. All employees with access to Veteran's health information are required to complete the Privacy and HIP AA Focused training as well as the VA Privacy and Information Security Awareness & Rules of Behavior training annually. The VA enforces two-factor authentication by enforcing smartcard logon requirements. PIV cards are issued to employees, contractors, and partners in accordance with HSPD-12. The Personal Identity Verification (PIV) Program is an effort directed and managed by the Homeland Security Presidential Directive 12 (HSPD-12) Program Management Office (PMO). IT Operations and Services (ITOPS) Solution Delivery (SD) is responsible for the technical operations support of the PIV Card Management System. Information is not shared with other agencies without a Memorandum of Understanding (MOU) or other legal authority.

Section 2. Uses of the Information

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

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

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

• Name: Used to identify the patient during appointments and in other forms of communication
• Social Security Number: Used as a patient identifier and as a resource for verifying income Information with the Social Security Administration
• Date of Birth: Used to identify age and confirm patient identity
• Mother's Maiden Name: Used to confirm patient identity
• Mailing Address: Used for communication, billing purposes and calculate travel pay
• Zip Code: Used for communication, billing purposes, and to calculate travel pay
• Phone Number(s): Used for communication, confirmation of appointments and conduct Telehealth appointments
• Fax Number: used to send forms of communication and records to business contacts, Insurance companies and health care providers
• Email Address: used for communication and MyHealtheVet secure communications
• Emergency Contact Information (Name, Phone Number, etc. of a different individual): Used in cases of emergent situations such as medical emergencies.
• Financial Account Information: Used to calculate co-payments and VA health care benefit eligibility
• Health Insurance Beneficiary Account Numbers: Used to communicate and bill third part Health care plans
• Certificate/License numbers: Used to track and verify legal authority to practice medicine and Licensure for health care workers in an area of expertise.
• Vehicle License Plate Number: Used for assignment of employee parking and assignment of parking during events
• Internet Protocol (IP) Address Numbers: Used for configuration and network connections. Network Communication allows information to be transferred from one Information Technology System to another.
• Current Medications: Used within the medical records for health care purposes/treatment, prescribing medications and allergy interactions.
• Previous Medical Records: Used for continuity of health care
• Race/Ethnicity: Used for patient demographic information and for indicators of ethnicity-related diseases.
• Tax Identification Number: Used for employment, eligibility verification
• Medical Record Number: Used to identify a patient within the medical record system without using their social security number as their identifier.
• Next of Kin: Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
• Guardian Information: Used when patient is unable to make decisions for themselves.

• Electronic Protected Health Information (ePHI): Used for history of health care treatment, during treatment and plan of treatment when necessary.
• Military history/service connection: Used to evaluate medical conditions that could be related to location of military time served. It is also used to determine VA benefit and health care eligibility.
• Service-connected disabilities: Used to determine VA health care eligibility and treatment plans/programs
• Employment information: Used to determine VA employment eligibility and for veteran contact, financial verification.
• Veteran dependent information: Used to determine benefit support and as an emergency contact person.
• Disclosure requestor information: Used to track and account for patient medical records released to requestors.
• Death certificate information: Used to determine date, location and cause of death.
• Criminal background information: Used to determine employment eligibility and during VA Police investigations.
• Education Information: Used for demographic background information for patients and as a determining factor for VA employment in areas of expertise. Basic educational background, e.g., High School Diploma, college degree credentials
• Gender: Used as patient demographic, identity, and indicator for type of medical care/provider and medical tests required for individual.
• Tumor PII/PID 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 Boundary sift through large amounts of information in response to a user inquiry or programmed functions. Facilities may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some facilities perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis facilities within the Boundary conduct and the data that is created from the analysis.

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

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

The VA Tuscaloosa uses statistics and analysis to create general reports that provide the VA a better understanding of patient care, benefits, etc.
These reports are:

1. Reports created to analyze statistical analysis on case mixes.
2. Analyze the number of places and geographical locations where patients are seen to assess the volume of clinical need.
3. Analyze appointment time-frame data to track and trend averages of time.

These reports may track:

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

VistA system uses statistics and analysis to create 3 types of general reports that provide the VA a better understanding of patient care and needs. These are reports are:

1. Reports created to analyze statistical analysis on case mixes.

2. Analyze the number of places and geographical locations where patients are seen to assess the volume of clinical need.

3. Track and trend appointment availability and length data to track and trend averages of 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. <u>Example: Describe if training for users of the project</u>

covers how to appropriately use information. Describe the disciplinary programs or Boundary controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

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

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

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

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

Section 3. Retention of Information

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

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

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

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

The Tuscaloosa VAMC Boundary itself, does not retain information.

- Name
- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Next to Kin
- Guardian Information
- Mailing Address
- ePHI
- Zip Code
- Phone Number(s)

- Fax Number
- Employment Information
- Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Disclosure requestor information
- Financial Account Information
- Health Insurance Beneficiary Numbers
- Tumor PII/PHI statistics
- Tax Identification Number
- Medical Record Number
- Account Numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Veteran dependance information

List additional SPI if applicable to your facility based on 1.1 above. (Examples below)

- Gender as provided by the patient
- Name and contact information for Guardian as provided by the patient
- Military and service history as provided by the patient and/or VBA
- Employment information as provided by the patient
- Veteran dependent information as provided by the patient
- Education information as provided by the patient
- Medical statistics for research purposes containing PII/PHI
- Name and contact information for Next of Kin
- Service-Connected rating and disabilities (based on information provided by Veteran and/or VBA)
- Date of death as supplied by Next of Kin or provider
- Criminal background and dependent information as reported by patient and/or national databases

3.2 How long is information retained by the facilities?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your Boundary may have a different retention period than medical records or education records held within your Boundary, please be sure to list each of these retention periods.
The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

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

- 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)l0-1, 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)l0-1, Part Three, Chapter Six- Healthcare Records, Item 6000.la. and 6000.l d.
- 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 lnformation & Technology (OI&T) Records: These records are created, maintained and disposed of in accordance with Department of Veterans Affairs, Office of lnfonnation & Technology RCS 005-1.

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 Boundary owner.

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

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

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

1, etc. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014) Additionally, the Tuscaloosa VAMC follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014, for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

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

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

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

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

Yes, where feasible to minimize the risk to privacy of using PII for research, testing, or training; no VA presentations or associated materials that may become publicly available shall contain PII or information exempt from release under the FOIA.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the Boundary.

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

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

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

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

Follow the format below:
Privacy Risk:

There is a risk that the information maintained by Tuscaloosa VAMC Vista System 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.

Mitigation:

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

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

Note: Question #3.5 (second table) in the Boundary Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT System***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT System***	***Describe the method of transmittal***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
Veterans Benefits Administration	Filing benefit claims	• Full Name • DOB • Social Security Number • Benefits	Compensation and Pension Record Interchange (CAPRI)	Area Tuscaloosa

		Information Claims Decision • DD-214	electronic software Package.	
Mid-Atlantic Consolidated Patient Account Center	Billing and Insurance services	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, • Account numbers	Electronically Transmitted	Area Tuscaloosa
VA Network Authorization Office- Non-VA Care Payments	Process authorizations for fee basis claims	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers Health insurance beneficiary numbers, Account numbers	Fee Basis Claim System (FBCS)	Area Tuscaloosa
VA Health Eligibility Center	Process Eligibility claims	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, 2) Account numbers	Electronically Transmitted	Area Tuscaloosa
Veterans Health Information Systems and Technology	Electronic Health Records	• Name • SSN, • DOB • Demographics	Secure FTP transmission, directlink between systems	Area Tuscaloosa

Architecture (VistA) & Computerized Patient Record System (CPRS)		• System Log files • Sample clinical data that may contain Protected Health Information (PHI)		
Human Resources	HR Management	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, Account numbers	Secure envelope	Area Tuscaloosa
Management Service	Electronic Personnel Records	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, • Account numbers	Electronically Transmitted	Area Tuscaloosa
Bryan Dorn VAMC	Business Partner for healthcare	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, Account numbers	VistA Mail and secure e-Mail	Area Tuscaloosa
Patient Advocate	Manages the feedback received from veterans,	• Full name • Social Security Number • DOB	Secure e-mail or verbal interview	Area Tuscaloosa

	family members and friends	• Email addresses • Medical record numbers • Phone Numbers • Health insurance • beneficiary numbers, Account numbers		
Chief of Staff	Monitoring and ensuring staff compliance with agency regulations; medical staff by-laws, rules and regulations; VA facility policies, Joint Commission standards and other regulations	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, • Account numbers Health Information (PHI), and Individually Identifiable Information (III).	Secure e-mail or verbal interview	Area Tuscaloosa
Central Alabama Health Care System CAVHCS	Business Partner for healthcare	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, Account numbers Health Information (PHI), and Individually Identifiable Information (III).	LEDI connection and physical manifest, sent by VA courier	CAVHCS
Lexington VAMC	Business Partner for healthcare	• Full name • Social Security Number • DOB • Email addresses	VistA mail and physical manifest, sealed sent by UPS	Lexington VAMC

		• Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, • Account numbers Health Information (PHI), and Individually Identifiable Information (III).		
Minneapolis VAMC	Business Partner for healthcare	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, Account numbers Health Information (PHI), and Individually Identifiable Information (III).	VistA mail and physical manifest, sealed sent by UPS	Minneapolis VAMC
Birmingham VAMC	Business Partner for healthcare	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance	Miscellaneous order form, sealed sent by VA courier	Birmingham VAMC

		beneficiary numbers, • Account numbers Health Information (PHI), and Individually Identifiable Information (III).		

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 internal sharing of data is necessary individuals to receive benefits at the Tuscaloosa VAMC. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

Mitigation:

Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a “least privilege/need to know” policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

Section 5. External Sharing/Receiving and Disclosure

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

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

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal

mechanism the facility is allowed to share the information in identifiable form or personally identifiable information outside of VA.

Note: Question #3.6 in the Boundary Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

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

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT System***	***List the specific data element types such as PII/PHI that are shared/received with the Program or IT System***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
TopCon	Provides health care to Veterans i.e., Optometry	• Name • Social Security Number • Date of Birth • Current Medications • Previous Medical Records • Race/Ethnicity • Medical Record Number • Electronic Protected Health Information (ePHI)	National ISA/ MOU	Secure Virtual VPN	DoD, Sharing VA to VA (Internal), and VA Health Eligibility Center

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT System***	***List the specific data element types such as PII/PHI that are shared/received with the Program or IT System***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
		• Military History/Service Connection • Service-connected Disabilities • Gender			
ScriptPro	Provides health care to Veterans i.e., Pharmacy	• Name • Social Security Number • Date of Birth • Current Medications • Previous Medical Records • Race/Ethnicity • Medical Record Number • Electronic Protected • Health Information (ePHI) • Military • History/Service Connection • Service-connected Disabilities • Gender	National ISA/ MOU	Secure Virtual VPN	DoD, Sharing VA to VA (Internal),
Phillips	Provide health care to Veterans	• Name • Social Security Number • Date of Birth • Current Medications • Previous Medical Records • Race/Ethnicity • Medical Record Number • Electronic Protected Health Information (ePHI) • Military History/Service Connection • Service-connected Disabilities • Gender	National ISA/ MOU	Secure Virtual VPN	DoD, Sharing VA to VA (Internal), and VA Health Eligibility Center

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)*
General Electric	Provide health care to Veterans	• Name • Social Security Number • Date of Birth • Current Medications Previous Medical Records • Race/Ethnicity • Medical Record Number • Electronic Protected Health Information (ePHI) • Military History/Service Connection • Service-connected Disabilities • Gender	National ISA/ MO	Secure Virtual VPN	DoD, Sharing VA to VA (Internal), and VA
CareFusion	Provide medical care to Veterans	• Name • Social Security Number • Date of Birth • Current Medications • Previous Medical Records • Race/Ethnicity • Medical Record Number • Electronic Protected Health Information (ePHI) • Military History/Service Connection • Service-connected Disabilities • Gender	National ISA/ MOU	Secure Virtual VPN	DoD, Sharing VA to VA (Internal), and VA Health Eligibility Center
Alere Informatics	Deliver details of diagnosis, infectious diseases, toxicology, and other solutions	• Name • Social Security Number • Date of Birth • Current Medications • Previous Medical Records • Race/Ethnicity	National ISA/ MOU	Secure Virtual VPN	DoD, Sharing VA to VA (Internal), and VA Health Eligibility Center

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT System***	***List the specific data element types such as PII/PHI that are shared/received with the Program or IT System***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
		• Medical Record Number • Electronic Protected • Health Information (ePHI) • Military • History/Service Connection • Service-connected • Disabilities • Gender			
Abbott	Deliver details of diagnosis, infectious diseases, toxicology, and other solutions	• Name • Social Security Number • Date of Birth • Current Medications • Previous Medical Records • Race/Ethnicity • Medical Record Number • Electronic Protected Health Information (ePHI) • Military History/Service Connection • Service-connected Disabilities • Gender	National ISA/ MOU	Secure Virtual VPN	DoD, Sharing VA to VA (Internal), and VA Health Eligibility Center
IRBnet	Aid Veterans through Research programs	• Health Insurance Beneficiary Numbers • Account numbers • Certificate/License numbers • Vehicle License Plate Number • Current Medications • Previous Medical Records • Race/Ethnicity • Tax Identification Number	National ISA/ MOU	Secure Virtual VPN	DoD, Sharing VA to VA (Internal), and VA Health Eligibility

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)*
		• Medical Record Number • Next of Kin • Guardian Information • Electronic Protected Health Information (ePHI) • Military History/Service Connection • Service-connected Disabilities • Employment Information • Veteran Dependent Information • Disclosure Requestor Information • Criminal Background • Education Information • Gender			

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)*
Department of Defense - DoD	Determine military service dates, eligibility	• 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 • Current Medications • Previous Medical Records • Race/Ethnicity • Tax Identification Number • Medical Record Number • Next of Kin • Guardian Information • Electronic Protected Health Information (ePHI) • Military History/Service Connection • Service-connected Disabilities • Employment Information • Veteran Dependent Information • Disclosure Requestor Information • Criminal Background • Education Information • Gender	National ISA/ MOU	Secure Virtual VPN	DoD, Sharing VA to VA (Internal), and VA Health Eligibility Center

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)*

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT System***	***List the specific data element types such as PII/PHI that are shared/received with the Program or IT System***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
Electronic Questionnaire for Investigators – E-QIP	Criminal background check Information such as basic demographics of name, date of birth, race, height and weight, plus previous criminal activity	• 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 • Current Medications • Previous Medical Records • Race/Ethnicity Tax Identification Number • Medical Record Number • Next of Kin • Guardian Information • Electronic Protected Health Information (ePHI) • Military History/Service	National ISA/ MOU	Secure Virtual VPN	DoD, Sharing VA to VA (Internal), and VA Health Eligibility Center

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)*
		Connection • Service-connected Disabilities • Employment Information • Veteran Dependent Information • Disclosure Requestor Information • Death Certification Information • Criminal Background • Education Information • Gender			

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)*
National Crime Information Center - NCIC	Criminal background check Information such as basic demographics of name, date of birth, race, height and weight, plus previous criminal activity	• 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 • Current Medications • Previous Medical Records • Race/Ethnicity • Tax Identification Number • Medical Record Number • Next of Kin • Guardian Information • Electronic Protected Health Information (ePHI) • Military History/Service Connection	National ISA/ MOU	Secure Virtual VPN	DoD, Sharing VA to VA (Internal), and VA Health Eligibility Center

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)*
		• Service-connected Disabilities • Employment Information • Veteran Dependent Information • Disclosure Requestor Information • Death Certification Information • Criminal Background • Education Information • Gender			

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 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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:

<u>Privacy Risk:</u>

The sharing of data is necessary for individuals to receive benefits at the Tuscaloosa VAMC. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

<u>Mitigation:</u>

Safeguards implemented to ensure data is not shared inappropriately with organizations are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know purposes, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption and access authorization are all measures that are utilized within the administrations. Standing letters for information exchange, business associate agreements and memorandums of understanding between agencies and VA are monitored closely by the Privacy Officer (PO), ISSO to ensure protection of information.

All personnel accessing Veteran's information must first have a successfully adjudicated background screening or Special Agreement Check (SAC). This background check is conducted by the Office of Personnel Management A background investigation is required commensurate with the individual's duties.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice in Appendix A. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Describe how the notice provided for the collection of information is adequate to inform those affected by the facilities within the Boundary that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

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

Site Type: VBA/VHA/NCA or Program Office	*Applicable SORs*
VHA	• Non-VA Fee Basis Records-VA, SOR 23VA10NB3 • Patient Medical Records-VA, SOR 24VA10A7 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA10 • Community Placement Program-VA, SOR 65VA122 • Health Care Provider Credentialing and Privileging Records-VA¸SOR 77VA10E2E • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10 • Income Verification Records-VA, SOR 89VA10NB

Site Type: VBA/VHA/NCA or Program Office	*Applicable SORs*
	• Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA131 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10 • National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147-VA10NF1VHA Corporate Data Warehouse- VA 172VA10A& • Health Information Exchange - VA 168VA005

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

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

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

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

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

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

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

The Tuscaloosa VAMC only requests information necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them.

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with Tuscaloosa VAMC.

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

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

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

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

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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:

<u>Privacy Risk:</u>

There is a risk that veterans and other members of the public will not know that the Tuscaloosa VAMC exists or that it collects, maintains, and/or disseminates PII, PHI or PII/PHI about them.

Mitigation:

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

Section 7. Access, Redress, and Correction

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

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

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

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

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

An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SOR. If an individual does not know the "office concerned," the request may be addressed to the PO of any VA field station VHA facility where the person is receiving care or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420. The receiving office must promptly forward the mail request received to the office of jurisdiction clearly identifying it as "Privacy Act Request" and notify the requester of the referral.

When requesting access to one's own records, patients are asked to complete VA Form 10-5345a: *Individuals' Request for a Copy of their Own Health Information*, which can be obtained from the medical center or online at https://www.va.gov/find-forms/about-form-10-5345a/.

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

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

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in **Appendix A**.

The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 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?

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

Follow the format below:

<u>Privacy Risk:</u>

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

<u>Mitigation:</u>

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

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

The Tuscaloosa VAMC Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.
The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

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

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

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

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

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

Individuals receive access to the Area Tuscaloosa by gainful employment in the VA or upon being awarded a contract that requires access to the boundary systems. Upon employment, the Office of Information & Technology (OI&T) creates computer and network access accounts as determined by employment positions assigned. Users are not assigned to software packages or network connections that are not part of their assigned duties or within their assigned work area. VA Tuscaloosa requires access to the GSS be requested using the local access request system. VA staff must request access for anyone requiring new or modified access to the GSS. Staff are not allowed to request additional or new access for themselves.

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

Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel. Access to computer rooms at VA Tuscaloosa is generally limited by appropriate locking devices and restricted to authorized VA IT employees. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at the health care area, or an OIG office location remote from the health care area, is controlled in the same manner.

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

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

- Individuals are subject to a background investigation before given access to Veteran’s information.

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

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

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

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

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

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

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

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

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

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

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

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

8.4a If Yes, provide:

1. *The Systems Security Plan Status: Please provide response here*
2. *The Systems Security Plan Status Date: Please provide response here*
3. *The Authorization Status: Please provide response here*
4. *The Authorization Date: Please provide response here*
5. *The Authorization Termination Date: Please provide response here*
6. *The Risk Review Completion Date: Please provide response here*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): Please provide response here*

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Section 9. References

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced Boundary Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**

ID	**Privacy Controls**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	Boundary of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
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.

MICHAEL CULVER Digitally signed by MICHAEL CULVER
Date: 2023.09.12 10:11:09 -05'00'

Privacy Officer, Michael Culver

Signature of Information System Security Officers

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

Shionell S. Williams
390217

Digitally signed by Shionell S. Williams
390217
Date: 2023.09.14 12:12:46 -05'00'

Information System Security Officer, Shionell Williams

Signature of Area Manager

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

BRYANT LEWIS Digitally signed by BRYANT LEWIS
Date: 2023.09.12 08:26:14 -05'00'

Area Manager, Bryant Lewis

APPENDIX A

Notice of Privacy Practices/VHA Privacy and Release of Information

Department of Veterans Affairs

CENTER MEMORANDUM NO. 00-13

VA Medical Center, Tuscaloosa, Alabama 35404

CENTER MEMORANDUM 00-13

September 4, 2021

PURPOSE I
POLICY II
RESPONSIBILITY III
PROCEDURES IV
REFERENCE V
RESCISSION VI
EXPIRATION DATE VII
PRIVACY POLICY

I. PURPOSE:

A. This memorandum implements facility privacy policy in compliance with Veterans Health Administration (VHA) Handbook 1605.1, Privacy and Release of Information Directive and establishes responsibilities and procedures for the privacy protection of information that is accessed, collected, maintained, used, disclosed, transmitted, amended and/or disposed of by the staff and systems of this facility.

B. The components in this policy are designed to meet all the specific requirements of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and Veteran Affairs and VHA policy. If any of the policy elements contained herein are removed, this facility policy will not be fully compliant.

C. In this document, the term workforce refers to on-site or remotely located employees, residents, students, Without Compensation (WOC) staff, volunteers, and any other appointed workforce members. Contractors will be held responsible for adhering to these policies and procedures in accordance with Contracts and Business Associate Agreements.

II. POLICY:

A. This facility will develop, implement, maintain, and enforce a structured privacy program to properly use, disclose and safeguard individually identifiable information. The privacy program is designed to allow continued operation of mission-critical activities while ensuring the integrity, availability, confidentiality and authenticity of data and information; minimum necessary access to protected health information; and a continuing awareness of the need for, and the importance of, information privacy within the facility.

1

B. All members of the workforce are responsible for complying with this privacy policy, applicable federal laws and regulations, VA and VHA policies, as well as the procedures and practices developed in support of these policies. All facility privacy policies and procedures must be consistent with VHA Directive 1605, BAA Handbook 1605.05 and VHA Handbooks series 1605.

C. All privacy and other workforce members responsible for implementing and complying with these policies and procedures will be provided copies of, or access to, this policy.

D. Violations of privacy policies or procedures will be brought to the attention of management for appropriate disciplinary action and/or sanctions and reported in accordance with national and local policy. Privacy violations will be reported through the Privacy and Security Event Tracking System (PSETS) to the VA Network and Security Operations Center (VA-NSOC) by the facility Privacy Officer within one hour of discovery during normal business or outside of normal business hours.

E. During non-business hours, violations will be reported to the Administrative Officer of the Day (AOD). The AOD will contact the Privacy Officer or designee with relevant details of any incident. If a privacy violation presents the risk of media involvement, congressional inquiry, legal action, immediate harm to any individual or any other high-risk outcome, the incident must be reported within one hour of discovery regardless of discovery time (even during non-business hours).

F All policies and procedures, and any actions/activities taken because of a privacy complaint/violation, must be documented in writing, and if applicable a written response letter must be given to the complainant. In addition to policies and procedures, privacy-related communications, decisions, actions and activities or designations, including any signed authorizations, must be documented and kept in a complaint file. All documentation must be retained in accordance with the VA Records Control Schedule (RCS-10).

G. All documentation related to the information privacy program will be reviewed and updated as needed in response to operational changes affecting the privacy of individually-identifiable information.

H The facility Privacy Officer (PO) is also the facility Freedom of Information Act (FOIA) Officer.

III. RESPONSIBILITY:

A. Executive Management (Director, Associate Director, Chief of Staff, Associate Director for Nursing and Patient Care Services) is responsible for:

1. Providing the necessary resources (funding and personnel) to support the Privacy Program, maintaining a culture of privacy, and ensuring that the facility meets all the privacy requirements mandated by VA/VHA policy and other federal legislation [e.g., Freedom of Information Act (FOIA) [5 U.S.C.§ 552], Health Insurance Portability and Accountability Act {HIPAA) Privacy Rule [45 C.F.R. Parts 160 and 164], Health Information Technology for Economic and Clinical Health (HITECH) Act, Privacy Act {PA) [5 U.S.C. §552a], VA Claims Confidentiality Statute [38 U.S.C. 5701], Confidentiality of Medical Quality Assurance Review Records [38 U.S.C. 5705] and Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection and Sickle Cell Anemia Medical Records [38 U.S.C. §7332].

2. Ensuring Privacy Officer's coverage for the facility and its associated clinics. II is required by VHA Privacy Policy that the facility Privacy Officer report directly to the Medical Center Director or Associate Director. When the facility Privacy Officer or Alternate is not available, provide coverage for off-hours operations if conducting 24/7 operations.

3. Ensuring facility Privacy Officers are fully involved in all projects concerning the access, collection, maintenance, use and/or disclosure, transmission, amendment and/or disposal of Ill.

4. Ensuring that new and revised Memorandums of Understanding (MOU), Contracts, Data Use Agreements (DUA), Business Associate Agreements (BAA), or similar agreements which involve the collection, transmission, use or sharing of information are reviewed by the facility Privacy Officer, in accordance with VAHandbook 6500.6, Contract Security, prior to approval by Executive Leadership.

2

5. Ensuring that the facility Privacy Officer is included in discussions and privacy concerns of the facility, which are addressed in strategic initiatives, and maintains a facility culture of privacy.

6. Cooperating with the facility Privacy Officer in any investigation, mediation strategies or correspondence that is required to investigate and resolve a complaint or allegation. Reports promptly to the VHA Privacy Office any potential privacy complaint, allegation or activity that has VISN level or national-level impact.

7. Certifying annually, or on an as needed basis, to the VHA Privacy Office, that privacy training has been completed for all personnel. This shall include all employees, volunteers, contractors, students, residents and any other person performing or conducting services on behalf of the facility.

8. Cooperating fully in submissions of Facility Self-Assessments (FSA) and On-site Privacy Compliance Assurance Assessments as required by the Privacy Compliance Assurance (PCA) Office.

9. Ensuring that facility employees exercise appropriate precautions and safeguards when discussing Veterans' individually identifiable information in public areas, such as clinic waiting rooms.

B. Privacy Officer is responsible for:

1 Developing, implementing, and updating local privacy policies and procedures. Conducting periodic assessments, compliance reviews and/or audits of the facility's collection, use, storage, and maintenance of personal information.

2. Conducting periodic assessments, compliance reviews and/or audits of the facility's collection, use, storage, and maintenance of personal information.

3. Establishing effective working relationships with the facility Information Security Officer, Facility Chief Information Officer (FCIO), Contracting Officer, Research Compliance Officer, Compliance Officer, and Human Resources Management personnel to ensure that local policies and procedures which may impact the privacy program support and complement each other.

4. Ensuring that Executive Leadership is apprised of all privacy related issues.

5. Coordinating with the facility Information Security Officer for the assurance of reasonable safeguards as required by the HIPAA Privacy Rule, HITECH, or other federal privacy statutes.

6. Serving as the facility's point of contact for matters relating to the privacy policies and procedures.

7. Ensuring that members of the workforce receive training and education about privacy policies and procedures as required by VHA Privacy Program.

8. Ensuring that members of the workforce know who to contact when a privacy complaint, incident or violation is identified or received.

9. Monitoring facility and workforce compliance with VHA privacy policies and procedures as well as compliance with local privacy policies and procedures.

10. Identifying and reviewing areas within the facility for auditory privacy risks, to ensure appropriate safeguards are in place to limit incidental disclosures.

11. Ensuring processes are in place for the appropriate accounting of disclosures of individually identifiable information made by the facility and appropriate utilization of the ROI Plus software or other tracking mechanisms are used in accordance with the facility's policies and procedures. The processes will include accounting for authorizations electronically conducted through i-Med Consent.

3

12. Collaborating with various program officials and the Contracting Officer, to ensure identification of all entities meeting the definition of Business Associates.

13. Maintaining a list of active Business Associates utilized by the facility and ensuring all Business Associates have a signed BAA in place prior to disclosure of individually identifiable health information (IIHI) and that the Business Associate adheres to the requirements of the BAA.

14. Ensuring that the facility does not maintain any unauthorized Privacy Act system of records.

15. Ensuring all facility developed paper, web-based or electronic forms that collect personal information contain the appropriate Privacy Act statements.

16. Reviewing and approving all MOUs, Contracts and/or DUAs when required for the sharing of VA sensitive data between the facility and other parties.

17. Ensuring prompt investigation and follow-up on allegations or known occurrences of privacy violations or complaints including logging the violation or complaint in the Privacy and Security Event Tracking System (PSETS). PSETS should be initiated upon notification of the violation during normal business hours, within one hour of discovery during normal business hours or as soon as possible outside of normal business hours. If a privacy violation presents the risk of media involvement, congressional inquiry, legal action, immediate harm to any individual or any other high-risk outcome, the incident must be reported within one hour of discovery regardless of discovery time (even during nonbusiness hours).

18. As a non-voting member of the facility IRB and R&D Committee, the Privacy Officer will review all human subject research protocols, exempt and non-exempt, in accordance with VHA Handbook 1200.05 and other applicable guidance to ensure legal authority exits prior to use and disclosure of VHA information for research.

19. Collaborating with the facility Information Security Officer, FCIO and System Owner to ensure that a Privacy Impact Assessment (PIA) is completed on all information technology systems, applications or programs that collect, maintain, and/or disseminate personally identifiable information (PII).

20. The Privacy Officer is to process requests, delete the "reviewing and processing" requirements of this section) Reviewing, processing, and monitoring requests to amend any information or record retrieved by an individual's name that is contained in a VA system of records, to include designated record sets, and coordinating such amendments with the author of the document.

21. Collaborating with the facility Information Security Officer, Contracting Officer Representative (COR) andthe Contracting Officer to ensure all contracts are reviewed in compliance with VA Handbook 6500.6.

22. Ensuring all facility's policies and procedures relating to HIPAA, HITECH, Privacy Act, 38 U.S.C.
§5701,- .. - §5705, and §7332, and FOIA are consistent with current guidelines and requirements, complementing and I. supporting each other.

23. Ensuring local departmental policies and procedures are developed if not specifically outlined in the '. facility privacy and FOIA policies.

24. Provide awareness training through various means for Veterans to inform them of their privacy rights and responsibilities.

25. Complete the Facility Self- Assessment by the last business day of each quarter or as required by PCA.

26. Ensuring that the reduction of SSN usage is reviewed to determine the necessity.

4

27. Other responsibilities as defined by the VHA Privacy Office.

C. FOIA Officer is responsible for:

1. Processing all FOIA requests for Federal records that would not otherwise be disclosed in accordance with HIPAA or the Privacy Act.

2. Ensuring that all FOIA requests or HIPAA/PA requests where information was withheld are entered FOIAXpress within the same day as receipt.

3. Other responsibilities as defined by the VHA FOIA Office.

4. Serving as FOIA Officer and PO at Tuscaloosa VA Medical Center.

D. Information Security Officer is responsible for:

1. Coordinating with the facility Privacy Officer for the assurance of reasonable safeguards as required by the HIPAA Privacy Rule, HITECH or other federal privacy statutes.

2. Coordinating, facilitating, and updating the establishment of information security policies and procedures, to work in tandem with privacy policies and procedures.

3. Establishing effective working relationships with the facility Privacy Officer, FCIO, Contracting Officer, Research Compliance Officer, Compliance Officer, and Human Resources Management personnel to ensure that information technology (IT) security and HIPAA/FOIA/PA/Federal Information Security Management Act (FISMA) policies and procedures compliment and support each other.

4. Reviewing and evaluating the security program impact(s) of any proposed facility information privacy policy and procedure changes.

5. Collaborating with the facility Privacy Officer on addressing/resolving privacy complaints, investigations, and access rights to audits and other information maintained by the facility Information Security Officer.

E. Clinical Staff or designees are responsible for:

1. Reviewing and determining appropriateness for granting individuals' requests for record amendment.

F. Facility Chief Information Officer (FCIO) or designee is responsible for:

1. Coordinating with facility Information Security Officer and facility Privacy Officer to provide technical adviceand other assistance relative to the reasonable safeguards requirements of privacy statutes and regulations dealing with implementation of IT systems, policies and procedures.

2. Identifying each locally maintained computer system that contains Ill and providing technical input forvarious mandated documents, reports, and investigations.

3. Ensuring all computer rooms meet acceptable reasonable safeguards and that minimum necessary access is maintained.

G Chief, Human Resources Management Service (HRMS), or designees are responsible for:

1. Providing guidance to supervisors and managers regarding personnel actions, sanctions, or other actions to be taken when employees have violated information privacy practices, laws, regulations, policies and procedures, and rules of behavior (see VA Directive 5021).

2. Providing appropriate information to facility Privacy Officer for completion of PSETS entries in a timelymanner.

3. Coordinating with facility Privacy Officer on the privacy of personnel records and other records maintained by HRMS.

4. Ensuring that personnel records maintained by the HRMS are maintained in compliance with applicable privacy policies, statutes, and regulations.

H. VA Contracting Officer/Contracting Officer Representative (COR) is responsible for:

1. Working in collaboration with the facility Privacy Officer to ensure that privacy responsibilities are listed inall contracts (see VA Directive 6500.6, Appendix C).

2. Ensuring through the COR that contractors are aware of, and abide by, those privacy responsibilities asstated in contracts with VA and VHA.

3. Ensuring that Business Associate Agreements are enacted for contracts which the contractor meets thedefinition of a Business Associate. A BAA should be a separate document from the contract.

4. Ensuring that contractors receive the appropriate privacy and if applicable security training upon initiation of the contract and annually thereafter.

5. Ensuring that contract performance meets privacy requirements including mediating and/or terminating the contract if information privacy requirements are not being met.

I. Local Managers, Supervisors, and their designees (e.g. ADPAC) are responsible for:

1. Identifying and protecting all individually identifiable information (Ill) used by supervised personnel, including contractors and other workforce members.

2. Ensuring that Ill, whether computerized or printed, is secured when work areas are unattended.

3. Training new personnel on roles and responsibilities for protecting Ill.

4. Identifying functional categories in accordance with facility policy and ensuring VA personnel have only theminimum necessary access level required to carry out their

authorized functions or assigned duties and that VA personnel understand what their minimal level of access is.

5. Ensuring applicable personnel complete the "Information Security and Privacy Awareness and Rules of Behavior" training. If access to protected health information (Pl:Il) is required then "Privacy and HIPAA" training must be completed within 30 days of hire or before access to PHI is given. Training must be completed annually thereafter and documented using the Talent Management System (TMS). Workforce members must be enrolled in TMS through either self-enrollment (e.g., contractors and volunteers) or automatic enrollment upon hire.

6. Ensuring that all media (paper, electronic, CDs, disks, portable devices, etc.) with Ill is disposed of via approved means in accordance with the VHA Records Control Schedule 10-1 and procedures outlined by the facility Records Management Officer.

6

7. Assists the facility Privacy Officer and Human Management Resource Service with the investigation and resolution of privacy incidents involving their employees and/or program(s).

J. Chief. Quality Management /QM) is responsible for:

1. Coordinating with the facility Privacy Officer on requests for copies of or access to QM documents. The facility Privacy Officer serves as the final approval authority for determining which documents are classified as quality management documents in accordance with VHA Directive 2008-077. Quality Management (QM) and Patient Safety Activities That Can Generate Confidential Documents prior to disclosure. The facility Privacy Officerwill work with the FOIA Officer concerning any exception to disclosure under FOIA.

K. Administrative Officer of the Day /AOD) is responsible for:

1. Resolving and responding to disclosure issues and incident reporting requirements consistent with VHA Directive 1605. VHA Handbooks 1605 series. VA Directive 6500 and VA Handbook 6500 series during non- business hours. The AOD will initiate preliminary investigation concerning any events and/or incidents and share all pertinent information with the Privacy Officer who will enter the ticket in the PSETS.

L. All individuals who have access to sensitive information are responsible for:

1. Accessing the minimum necessary data for which they have authorized privileges and on a need-to- knowbasis in the performance of their official VA duties.

2. Protecting an individual’s rights to privacy and ensuring proper use and disclosure of information. All workforce members will be held accountable for compliance with these policies. procedures. and applicable laws.

3. Appropriately safeguarding printed and electronic individually identifiable information.
4. Reporting complaints and/or violations of privacy policies or procedures to the facility Privacy Officerimmediately upon discovery.
5. Consulting the facility Privacy Officer and VHA Handbook 1605.1 for guidance in privacy situations notaddressed in this document.

6. Adhering to the facility Clean Desk Policy

7. Adhering to the facility Authorization to Transport Sensitive Information

M. Content Update Responsibility:

1. Privacy/Freedom of Information Act Officer, Associate Director.

IV.- PROCEDURES: The Glossary of Terms and Acronyms are provided in the VHA Privacy and Procedures Policy

V. REFERENCES: VHA Directive 1605, VHA Privacy Program; VHA Handbook 1605.1, Privacy and Release of Information; VHA Handbook 1605.2, Minimum Necessary Standard for Protected Health Information; VHA Directive 2009-013, Confidential Communications; VHA Directive 2003-024; Fact Sheet: Facility Directory Opt-Out; VHA Handbook 1600.01 Business Associate Agreements; VHA Directive 2008-071, October 29. 2008, Provision of Medical Statements and Completion of Forms by VA Health Care Providers; Department of Veterans Affairs Office of Information and Technology, Formal Event Review and Evaluation Tool (FERET) User's Guide May 2007; Department of Veterans Affairs VA Privacy Service April 2007; Privacy Violation Tracking System Basic User's Manual; Center Memorandum

7

00-12, Information Security Policy; VHA Handbook 1605.04, Notices of Privacy Practices; VA Directive 6300, Records and Information Management; VA Directive 6502, Privacy Program; and VA Handbook 6300.3, Procedures for Implementing the Freedom of Information Act

VI. RESCISSIONS: Center Memorandum 00-13 dated January 28, 2014
VII. EXPIRATION DATE: Mandatory Review Date: March 2020
VII. Mandatory Update: September 2021

Charles Gills, MSN, RN, FNP-BC,
Acting Director

Attachment A: Privacy Policy DISTRIBUTION B

APPENDIX B – PII Mapped to Components

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

Components of the Boundary collecting/storing PII *(Each row refers to a grouping of databases associated with a single server)*	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
Server 1 • BHL_TUA_Prod • BHL_TUA_Test • BIORAD_LAB • Censis_Beta_V2_Global • censis_graphics • Censis_HL1952 • Censis_SG1952 • CensisBufferAgent • CLIQRemote • CLIQWeb • CompassTUA • EMR • IntelliWare • JCIAuditTrails • JCIEvents • JCIHistorianDB • JCIItemAnnotation • JCIReportingDB • master • MetasysFault • MetasysFaultTriage	Yes	Yes	Yes	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, Account numbers	To ensure the integrity of PII is set to VA standards.	• Encrypted AES 256 • System Database • Encrypted Asymmetric Key	Area Tuscaloosa

Components of the Boundary collecting/storing PII *(Each row refers to a grouping of databases associated with a single server)*	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
• MetasysIII • MetasysReporting • MetasysTranslationDictionary • MetasysValue • model • msdb • NOAHDatabaseCore • PSESCoreDB • PSESCoreTab • PSESDBNetCare • PSESJlcDB • RDTWeb • ReportServer_TEMPTRAK • ReportServer_TEMPTRAKTempDB • RightFax20 • Romexis_db • SFFX • SpacesAuthorization • SystemState • tempdb • TUA_BioPoint_PI6 • WADB-INP • WADB-OUTP • XMS							

Components of the Boundary collecting/storing PII *(Each row refers to a grouping of databases associated with a single server)*	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
Server 2 • ACVSAudit • ACVSBIRS • ACVSCore • ACVSJournal • ACVSUJournal_00010002 • ACVSUJournal_00010003 • ACVSUJournal_00010004 • ACVSUJournal_00010005 • ACVSUJournal_00010006 • ACVSUJournal_00010007 • ACVSUJournal_00010008 • ACVSUJournal_00010009 • ACVSUJournal_00010010 • ACVSUJournal_00010011 • ACVSUJournal_00010012 • DRSVHATUA • master • model • msdb • pivCLASS • SmartLink • SWHSystemAudit • SWHSystemJournal • SystemState • tempdb • VHATUAOuputManData	Yes	Yes	Yes	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, Account numbers	To ensure the integrity of PII is set to VA standards.	• System Database • Encrypted Asymmetric Key • Encrypted AES 256	Area Tuscaloosa

***Components of the Boundary collecting/storing PII** (Each row refers to a grouping of databases associated with a single server)*	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
Server 3 • Lynx • master • model • msdb • SystemState • tempdb	Yes	Yes	Yes	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, Account numbers	To ensure the integrity of PII is set to VA standards.	• System Database • Encrypted AES256 • Encrypted Asymmetric Key	Area Tuscaloosa
Server 4 • master • model • msdb • SystemState • tempdb	Yes	Yes	Yes	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, Account numbers	To ensure the integrity of PII is set to VA standards.	• System Database • Encrypted AES256 Encrypted Asymmetric Key	Area Tuscaloosa
Server 5 (Access 3000) • A3k • master • model • msdb • SystemState	Yes	Yes	Yes	• Full name • Social Security Number • DOB • Email addresses • Phone Numbers	To ensure the integrity of PII is set to VA standards.	• Bitlocker Encrypted AES 256 • System Database	Area Tuscaloosa

***Components of the Boundary collecting/storing PII** (Each row refers to a grouping of databases associated with a single server)*	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Applicable Sites within Boundary (VBA, VHA, NCA, Program Office)***
• tempdb						• Encrypted Asymmetric Key	
Server 6 (UPS Worldship) • master • model • msdb • SystemState • tempdb • Upslpmdb • UPSNrfRVLDB • UPSNrfUserDB • upswsdb • upswsdb_ActivityLog • upswsdb_reconciler • upswsdb_report	Yes	Yes	Yes	• Full name • Social Security Number • DOB • Email addresses • Medical record numbers • Phone Numbers • Health insurance beneficiary numbers, Account numbers	To ensure the integrity of PII is set to VA standards.	• Bitlocker Encrypted AES 256 • System Database • Encrypted Asymmetric Key	Area Tuscaloosa

APPENDIX C – List of Medical Devices and Special Purpose Systems

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