Date PIA submitted for review:

April 9, 2024

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

Area Ann Arbor

Midwest District

---

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

Sites within Area:

Sites	Station Numbers
1) VHA Medical Center Ann Arbor Healthcare System (HCS)	506
2) Field Program Office National Center for Patient Safety (NCPS)	899
3) Flint Community Based Outpatient Clinic	506GB
4) Jackson Adrian Community Based Outpatient Clinic	506GC
5) Toledo Community Based Outpatient Clinic	506GA
6) Adrian Community Based Outpatient Clinic	506GF
7) Packard Road Adrian Community Based Outpatient Clinic	506
8) Green Road Adrian Community Based Outpatient Clinic	506
9) North Campus Research Complex (NCRC)	N/A
10) Toledo Vet Center	N/A
11) Toledo Annex	N/A
12) An Ann Arbor Off-Site Warehouse	N/A
13) Huron Towers Administration Office	N/A
14) VISN 10 Contracting Office Ann Arbor	N/A
15) Readjustment Counseling Service (RCS) Ann Arbor	N/A
16) Canton Community Based Outpatient Clinic	506GD
17) Howell Community Based Outpatient Clinic	506GE

Area Contacts:

Area Key Stakeholders

Name	Title (PO, ISSO, AM)	Phone Number	Email Address	Applicable Site (VBA, VHA, NCA, Program Office)
Designated PO: Verona Robinson	Privacy Officer	734-845-5314	Verona.Robinson @va.gov	VHA
Malinda Williams	Assistant Privacy Officer	734-845-3556	Malinda.Williams1 @va.gov	VHA

Name	Title (PO, ISSO, AM)	Phone Number	Email Address	Applicable Site (VBA, VHA, NCA, Program Office)
David Jones	Information System Security Officer	734-263-9622	David.Jones9@va.gov	VHA
John Kucans	Area Manager	734-222-4334	John.Kucans@va.gov	VHA

Abstract

The abstract provides the simplest explanation for "what does the Area do?".

Area Ann Arbor is an Information Area that consists of VHA Ann Arbor Healthcare Systems (HCS), Field Program Office National Center for Patient Safety (NCPS), Flint Community Based Outpatient Clinic, Jackson Community Based Outpatient Clinic, Toledo Community Based Outpatient Clinic, Adrian Community Based Outpatient Clinic, Canton Community Based Outpatient Clinic, Howell Community Base Outpatient Clinic, Packard Road Community Based Outpatient Clinic, Green Road Community Based Outpatient Clinic, North Campus Research Complex, Toledo Vet Center, Toledo Annex, VA Ann Arbor Off-Site Warehouse, Huron Towers Administration Office, and VISN 10 Contracting Office Ann Arbor. The Area environment consists of components such as workstations, laptops, portable computing devices, terminals, servers, printers, and IT enabled networked medical devices that are owned, managed, and maintained by the facilities. The Area provides operational connectivity services necessary to enable users' access to information technology resources throughout the enterprise including those within the facility, between facilities, resources hosted at data centers, and connectivity to other systems. Network connectivity rules are enforced by VA approved baselines for router and switch configurations. The Area system environment also includes as applicable, subsystem storage utilities such as tape drives, optical drives, disk drives, network attached storage (NAS), storage area networks (SAN), archival appliances, special purpose systems, and tier 2 storage solutions. The Area encompasses the management, operational, and technical security controls associated with IT hardware, consisting of servers, routers, switches, hubs, gateways, peripheral devices, desktop/laptops, and OS software. The Area employs a myriad of routers and switches that connect to the VA network.

Special Purpose Systems are non-medical, non-research VA network-connected, and non-Office of Information and Technology (OIT) supported Operational Technology (OT) device/system that cannot obtain a VA approved baseline.

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

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

The Area Ann Arbor itself does not collect, use, disseminate, maintain, or store PII/PHI.
VHA, VBA and NCA Facilities located within the Area Ann Arbor IT Area all access VA Enterprise IT systems respectively, hosted and maintained outside of this Area. These are VISTA, Veterans Benefits Management System (VBMS), Memorial Benefits System (MEM), etc.

Special Purpose Systems consists of specialized devices, and applicable components, hosted within the facilities associated to the Area. The system environment is comprised of operational technology devices/systems that assist, support, and maintain mission capabilities and operations for building safety, healthcare services, security services and other general services functional support areas.

The system environment may include, but are not limited to; energy management systems, heating ventilation and air conditioning (HVAC), temperature controls, building/facility access controls, building automation systems, utility control systems, distributed control systems, security cameras, emergency response vehicle dashcams, Virtual Reality (VR) headsets, promethean boards, TUG robots, Telesitter, and other business Operational Technologies. All Special Purpose Systems are identified in **Appendix C**.

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

The facilities within the Area collect, use, and/or disseminate PII/PHI that is maintained and stored within enterprise systems such as VistA, Veterans Benefits Management System (VBMS), Burial Operations Support System (BOSS)/ Automated Monument Application System (AMASS), etc. There are individual PIAs that contain detailed information on the maintenance, dissemination and sharing practices, and storage of the PII/PHI for each Enterprise system accessed by the facilities.

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

The applicable SORs for Area Ann Arbor include:

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	Applicable System of Records (SORs)
*VHA	• Non-VA Fee Basis Records-VA, SOR 23VA10NB3

Site Type: VBA/VHA/NCA or Program Office	Applicable System of Records (SORs)
	• Patient Medical Records-VA, SOR 24VA10A7 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA10 • 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 89VA10 • 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 121VA10 • Enrollment and Eligibility Records- VA 147VA10NF1 • VHA Corporate Data Warehouse- VA 172VA10 • Health Information Exchange - VA 168VA005

Section 1. Characterization of the Information

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

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

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

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

Please check any information listed below that the facilities within the Area 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)
☒ 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
☒ Other Unique Identifying Numbers
☒ Gender
☒ temporary mailing address and telephone numbers
☒ Name and contact information for Personal Representative
☒ Guardian and Beneficiaries
☒ Name and contact information for Next of Kin

☒ Employment information
☒ Education information
☒ Medical statistics for research purposes containing PII/PHI
☒ Military and service history
☒ Veterans rated disabilities
☒ Criminal background and dependent information
☒ Date of death as supplied by Next of Kin or provider
☒ Claims decision,
☒ DD – 214
☒ Benefits information
☒ System log files
☒ Sample clinical dates that may contain PHI
☒ Demographics

☒ Diagnoses
☒ Death certificates
☒ Veteran eligibility
☒ Procedures
☒ Tumor status
☒ Treatment outcome
☒ Survivor tracking
☒ Type of treatments
☒ Problem Lists
☒ Diagnosis and procedures
☒ Human Immunodeficiency Virus/Acquired Immunodeficiency Virus (HIV/AIDS) status, treatment outcomes

PII Mapping of Components (Servers/Database)

Area Ann Arbor consists of 66 key components (server/database) 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 Ann Arbor and the reasons for the collection of the PII are in the **Mapping of Components Table in Appendix B of this PIA.**

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

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

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

The information that resides within the facilities in the Area is collected, maintained, and/or disseminated comes from a variety of sources. The largest amount of data comes directly from individuals - including veterans and their dependents, volunteers and other members of the

public, clinical trainees, and VA employees and contractors. For example: items such as names, social security numbers, dates of birth are collected from the individual on healthcare enrollment forms (VA Form 10-10EZ), or other paperwork the individual prepares. An application for employment contains the same, or similar, information about employees.

Depending on the type of information, it may also come from Veterans Benefits Administration (VBA), the VA Health Eligibility Center (HEC), VA Network Authorization Office (NAO) for non-VA Care payments, and non-VA medical providers, Department of Defense (DOD), Internal Revenue Service (IRS), Office of Personnel Management (OPM), Social Security Administration (SSA), Federal Emergency Management Agency (FEMA), Federal Bureau of Investigation (FBI).

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

1.3 How is the information collected?

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

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

Means of Collection Table

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

Site Type: VBA/VHA/NCA or Program Office	Means of Collection
	information provided by veterans or other members of the public, such as address and phone number, next of kin and emergency contact information, and similar information are assumed to be accurate because it is provided directly by the individual. Additionally, information entered into an individual's medical record by a doctor or other medical staff is also assumed to be accurate.

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

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

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

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

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

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

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

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

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
NCPS	• 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 healthcare workers to practice medicine and/or subject matter expertise • Responding to release of information request • Third party health care plan billing, e.g. private insurance • Statistical analysis of patient treatment • Contact for employment eligibility/verification

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

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

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

Information that is collected and used directly from enterprise systems have additional details regarding checks for accuracy in their own enterprise level PIAs.

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

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

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

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

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

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

Legal Authority Table

Site Type: VBA/VHA/NCA or Program Office	Legal Authority
*VHA	• Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a) • Health Insurance Portability and Accountability Act of 1996 (HIPAA) • Privacy Act of 1974 • Freedom of Information Act (FOIA) 5 USC 552 • VHA Directive 1605.01 Privacy & Release of Information • VA Directive 6500 Managing Information Security Risk: VA Information Security Program.
NCPS	• Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a) • Health Insurance Portability and Accountability Act of 1996(HIPAA)

	• Privacy Act of 1974
	• Freedom of Information Act (FOIA) 5 USC 552
	• VHA Directive 1605.01 Privacy & Release of Information
	• VA Directive 6500 Managing Information Security Risk: VA Information Security Program.

1.7 **PRIVACY IMPACT ASSESSMENT: Characterization of the information**

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:
VA Area Ann Arbor collects Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation:
VA Area Ann Arbor employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control, awareness and training, audit and accountability, certification, accreditation, and security assessments, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and

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

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

Section 2. Uses of the Information

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

2.1 Describe how the information within the Area 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,
- **Personal Mailing Address**: Used for communication, billing purposes and calculate travel pay,
- **Personal Phone Number(s):** Used for communication, confirmation of appointments and conduct Telehealth appointments,
- **Personal Fax Number**: used to send forms of communication and records to business contacts, Insurance companies and health care providers,
- **Personal 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.

- **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,
- **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.
- **Other Unique Identifying Numbers:** Used as a patient identifier and as a resource for verifying income Information,
- **Gender**: Used as patient demographic, identity and indicator for type of medical care/provider and medical tests required for individual.
- **Temporary Mailing Address and Telephone numbers:** Used for communication, billing purposes and calculate travel pay,
- **Name and contact information for Personal Representative:** Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
- **Name and Contact information for Next of Kin**: Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
- **Guardian and beneficiaries Information**: Used when patient is unable to make decisions for themselves.
- **Employment information**: Used to determine VA employment eligibility and for veteran contact, financial verification.
- **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
- **Medical Statistics for Research Purposes Containing PHI/PII:**
- **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.
- **Veteran Rated Disabilities:** Used for billing purposes and calculate travel pay,
- **Criminal background and dependent information:** Used to determine employment eligibility and during VA Police investigations.
- **Claims decision:** Used for billing purposes and calculate travel pay,
- **DD – 214:** Used to identify the patient and eligibility of benefits,

- **Benefit Information**: Used to verify burial benefits,
- **System log files:** Used for continuity of health care,
- **Sample clinical dates that may contain PHI:** Used for continuity of health care,
- **Demographics:** Used for communication, billing purposes and calculate travel pay,
- **Diagnoses:** Used to evaluate medical conditions and determine treatment plan,
- **Death certificate information**: Used to determine date, location and cause of death.
- **Date of Death as supplied by Next of Kin or provider**: Used to verify spousal and beneficiary relationship to Veteran, at time of death,
- **Veteran eligibility:** billing purposes and calculate travel pay,
- **Procedures:** Used to evaluate medical conditions and determine treatment plan,
- **Tumor PII/PHI Statistics**: Used to evaluate medical conditions and determine treatment plan,
- **Treatment outcome:** Used to evaluate medical conditions and determine treatment plan,
- **Survivor tracking:** Used to determine benefit support and as an emergency contact person.
- **Type of treatments:** Used to evaluate medical conditions and determine treatment plan,
- **Problem Lists:** Used to evaluate medical conditions and determine treatment plan,
- **Diagnosis and procedures:** Used to evaluate medical conditions and determine treatment plan,
- **Human Immunodeficiency Virus/Acquired Immunodeficiency Virus (HIV/AIDS) status, treatment outcomes:** Used to evaluate medical conditions and determine treatment plan.

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

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

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

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

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

The VA Area Ann Arbor uses statistics and analysis to create general reports that provide the VA a better understanding of patient care, benefits. 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

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

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

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

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

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

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

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

Section 3. Retention of Information

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

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

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

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

The Area Ann Arbor itself, does not retain information.

- 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)
- Health Insurance Beneficiary Account Numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number

- Medical Record Number
- Other Unique Identifying Numbers
- Gender
- Temporary Mailing Address and Telephone numbers
- Name and contact information for Personal Representative
- Name and Contact information for Next of Kin
- Guardian and beneficiaries Information
- Employment information
- Education Information
- Medical Statistics for Research Purposes Containing PHI/PII
- Military history/service connection
- Veteran Rated Disabilities
- Criminal background and dependent information
- Claims decision
- DD – 214
- Benefit Information
- System log files
- Sample clinical dates that may contain PHI,
- Demographics
- Diagnoses
- Death certificate information
- Date of Death as supplied by Next of Kin or provider,
- Veteran eligibility
- Procedures
- Tumor PII/PHI Statistics
- Treatment outcome
- Survivor tracking
- Type of treatments
- Problem Lists
- Diagnosis and procedures
- Human Immunodeficiency Virus/Acquired Immunodeficiency Virus (HIV/AIDS) status, treatment outcomes.

3.2 How long is information retained by the facilities?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your Area may have a different retention period than medical records or education records held within your Area, please be sure to list each of these retention periods.

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

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

Length of Retention Table

Site Type: VBA/VHA/NCA or Program Office	Length of Retention
*VHA	• Financial Records: Different forms of financial records are retained 1-7 years based on specific retention schedules. Please refer to VA Record Control Schedule (RCS)10-1, Part Two, Chapter Four- Finance Management • Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)10-1, Part Three, Chapter Six-Healthcare Records, Item 6000.1a. and 6000.1d. • Official Human Resources Personnel File: Folder will be transferred to the National Personnel Records Center (NPRC) within 30 days from the date an employee leaves the VA. NPRC will destroy 65 years after separation from Federal service. (Department of Veterans Affairs Record Control Schedule (RCS)10-1, Part Two, Chapter Three- Civilian Personnel, Item No. 3000.1 • Office of Information & Technology (OI&T) Records: These records are created, maintained and disposed of in accordance with Department of Veterans Affairs, Office of Information & Technology RCS 005-1.
NCPS	• Financial Records: Different forms of financial records arere trained 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 theVA.NPRC will destroy 65 years after separation from Federal service. (Department of Veterans Affairs Record Control Schedule (RCS)10-1, Part Two, Chapter Three- Civilian Personnel, Item No. 3000.1 • Office of Information & Technology (OI&T) Records: These records are created, maintained and disposed of in accordance with Department of Veterans Affairs, Office of Information &Technology RCS 005-1.

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

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

Retention Schedule Table

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

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

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

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

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

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

3.5 Does the Area 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

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by Area Ann Arbor could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation: To mitigate the risk posed by information retention, Area Ann Arbor adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. The Area Ann Arbor ensures that all personnel involved with the collection, use and retention of data are trained in the correct process for collecting, using and retaining this data. A Records Management Officer (RMO), Privacy Officer (PO) and an Information System Security Officer (ISSO) are assigned to the Area to ensure their respective programs are understood and followed by all to protect sensitive information form the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning the proper handling of information.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations are facilities within the Area 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 Area Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

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

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared/received with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT System*	*Describe the method of transmittal*	*Applicable Sites within Area (VBA, VHA, NCA, Program Office)*
VistA	Patient Care	Area Boundary Log files, sample clinical data that may contain Protected Health Information (PHI)	Electronically pulled from VistA thru Computerized Patient Record Area Boundary (CPRS)	VHA
Veterans Benefits Administration	Patient Care	Personally Identifiable Information (PII), Protected Health Information (PHI), and	Compensation and Pension Record	VHA

List the Program Office or IT System information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT System	List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT System	Describe the method of transmittal	Applicable Sites within Area (VBA, VHA, NCA, Program Office)
		Individually Identifiable Information (III).	Interchange (CAPRI) electronic software package	
Data Services	Patient Care	Personally Identifiable Information (PII), Protected Health Information (PHI), Individually Identifiable Information (III), System Logfiles, sample clinical data that may contain Protected Health Information (PHI)	SOAP over HTTPS using SSL encryption and Certificate exchange	VHA
National Cemetery Administration	Patient Care	Death certificates, veteran eligibility	hard copy mailing	VHA
Health Eligibility Center	Patient Care	Name, Date of Birth, Sex, SSN, demographics, and health information	Information may be transmitted electronically	VHA
Austin Automation Center	Patient Care	Name, date of birth, sex, SSN, demographics, health information	Information may be transmitted electronically. AAC employees can log VA Tumor Registry	VHA
VA Tumor/Cancer Registry	Patient Care	Diagnosis and procedures, tumor status, treatment outcome, survivor tracking, type of treatments, demographics, problem lists	Electronic tumor registry package	VHA
HIV, Hepatitis, and Related Conditions Programs	Patient Care	Diagnosis and procedures, Human Immunodeficiency Virus/Acquired	Electronic Human Immunodeficiency Virus (HIV) registry package	VHA

List the Program Office or IT System information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT System	List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT System	Describe the method of transmittal	Applicable Sites within Area (VBA, VHA, NCA, Program Office)
		Immunodeficiency Virus HIV/AIDS) status, treatment outcomes, survivor tracking, type of treatments, demographics, problem lists		
VA network authorization office – Non-VA Care payments	Patient Care	Demographics, diagnoses, medical history, service connection, provider orders, Veterans Health Administration (VHA) recommendation/approval for non-VA care.	Fee basis claim system (FBCS) authorization software program	VHA
Consolidated Mail Outpatient Pharmacy	Patient Care	Veteran's name, address, full SSN, DOB, provider's name, name/quantity of medication(s)	Veterans Information Systems and Technology	VHA
National Veteran's Service Organizations – specific organizations such as Veterans of Foreign War (VFW), etc.	Patient Care	Name, Social Security Number, Date of Birth, Mailing Address, Phone Numbers, Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers, Current Medications, Previous Medical Records and Race/Ethnicity as appropriate to the request	Electronically, verbal, or written in a sentence format. For example, Information may be transmitted upon request in an electronic, written, or verbal format based on the individual request	VHA
Department of Veterans Affairs General Counsel Office	Patient Care	Name, Social Security Number, Date of Birth, Mailing Address, Phone Numbers, Email Address, Emergency Contact Information, Financial Account Information, Health Insurance	Electronically, verbal, or written in a sentence format. For example, Information may be transmitted upon request in an	VHA

List the Program Office or IT System information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT System	List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT System	Describe the method of transmittal	Applicable Sites within Area (VBA, VHA, NCA, Program Office)
		Beneficiary Numbers, Current Medications, Previous Medical Records and Race/Ethnicity as appropriate to the request	electronic, written, or verbal format based on the individual request	

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 Area Ann Arbor. 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 Area Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VBA, VHA, NCA, Program Office)*
Office of Personnel Management (OPM)	Employment Information	Name, Date of Birth, Sex, SSN, demographics, and employment information.	National ISA/MOU	Information may be transmitted upon request in an electronic, written or verbal format based on the individual request. Secure facsimile or hard copies via routine mail.	VHA
Health Information Exchange – VA	Veteran Health Information	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable information (III) Name, Date of Birth, Sex, SSN, demographics, and employment information.	168VA005	Electronic via EDI interface	VHA
Ohio Department of Job and Family Services	Veterans or family when suspicion of elder or child	Name, date of birth, Sex, SSN, demographics, and employment information	Standing letter to comply with	Secure fax or phone	VHA

			Article 6, Chapter 108A of NC General Statutes		
Department of Health and Human Services Adult Protective Services (APS) and Child Protective Services (CPS	Veterans or family when suspicion of elder or child abuse or neglect.	Name, date of birth, SSN, demographics regarding veterans or family when suspicion of elder or child abuse or neglect.	Standing letter to comply with Article 6, Chapter 108A of NC General Statutes	Secure fax or phone	VHA
Internal Revenue Service (IRS)	Employment and Veteran Information	Name, Date of birth, sex, SSN, demographics.	ISA/ MOU, VA Privacy Act 1974;	Secure Web-Portal, Secure Socket Layer	VHA
Federal Bureau of Investigation (FBI)	National Security	Name, Date of birth, sex, SSN, demographics.	VA SORN 02VA135 VA SORN 79VA10	Secure Web-Portal, Secure Socket Layer	VHA
Department of Defense (DoD)	Veteran Health Information	Read only access to health information for plan treatments, Name, Date of Birth, SSN, demographics, Protected Health Information (PHI), benefits/copay information, IP Address	ISA MOU	Site to Site VPN	VHA
Veterans Health Information Exchange (VHIE)	Veteran Health Information	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) Name, Date of	Restatement II of the Data Use and Reciprocal Support Agreement	eHealth Exchange	VHA

		Birth, Sex, SSN, demographics			
Change Health Care (Formally McKesson)	Veteran Healthcare	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) Name, Date of Birth, Sex, SSN, demographics	MOU National	Site to Site VPN	VHA
Omnicell	Veteran Healthcare	The expected benefit of the interconnection is to expedite the processing of data associated with remote diagnostics, maintenance, monitoring, and repair for the Omni Center or Work Flow Rx Server withing prescribed timelines.	National MOU	Transmitted upon request in an electronic, written, or verbal format based on the individual request	VHA
GE Healthcare	Veteran Healthcare	The expected benefit of the interconnection is to expedite the processing of data associated with remote diagnostics, maintenance, monitoring, and repair for the GE Healthcare Systems within prescribed timelines	National MOU	Site to Site	VHA

ScriptPro	Veteran Healthcare	To allow ScriptPro to expedite the processing of data associated with remote diagnostics, maintenance, monitoring, and repair by ScriptPro's technical support services for the ScriptPro SPCentral Systems installed in VA facilities. The Syngo Lab Manager and Syngo Lab Connectivity Manager provide diagnostics capabilities for laboratory patient results and order management. The purpose of this connection is to allow Siemens staff to access the VA siemens medical devices to remotely diagnose, repair and monitor and update siemens medical devices. Pertinent Personally Identifiable Information PHI To expedite the processing of data associated	National MOU	Site to Site	VHA

		with remote diagnostics,			
Topcon	Veteran Healthcare	Processing of data associated with remote diagnostics, maintenance, monitoring, quality control program and repair by Topcon Medical Systems support service for the IMAGEnet Imaging System.	National MOU	Site to Site	VHA
Siemens	Veteran Healthcare	The Syngo Lab Manager and Syngo Lab Connectivity Manager provide diagnostics capabilities for laboratory patient results and order management. The purpose of this connection is to allow Siemens staff to access the VA siemens medical devices to remotely diagnose, repair and monitor and update siemens medical devices.	National MOU	Site to Site	VHA
Department of Health and Human Services Infectious Disease	Veteran Healthcare Healthcare	Name, date of birth, SSN, demographics, diagnosis, treatment, and follow-up, regarding Veterans	Standing with Article 6, Chapter General Statutes	Secure fax or phone	VHA

		contracting infectious disease listed under mandated State infectious diseases.			
Philips Healthcare	Veteran Healthcare	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III) Name, Date of birth, sex, SSN, demographics.	National ISA/MOU	Site to Site	VHA
Quest Diagnostics	Veteran Healthcare	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Name, Date of birth, sex, SSN, demographics.	National ISA/MOU	Site to Site	VHA
AGFA	Veteran Healthcare	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable	National ISA/MOU	Site to Site	VHA

		Name, Date of birth, sex, SSN, demographics.			
Vecna	Veteran Healthcare	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Name, Date of birth, sex, SSN, demographics.	National ISA/MOU	Site to Site	VHA
Sysmex	Veteran Healthcare	To expedite the processing of data associated with remote diagnostics, maintenance, monitoring, quality control program and repair for sysmex clinical laboratory instruments within the prescribed timelines. Pertinent Personally Identifiable	National MOU	Site to Site	VHA
Michigan Dept. of Licensing and Regulatory Affairs (LARA)	Veteran Healthcare	Pertinent Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable	Standing letter to comply with Article 6, Chapter 108A of NC General Statutes	Secure fax or phone	VHA

		Information (III Name, Date of birth, sex, SSN, demographics.			

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

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

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

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure
Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

Follow the format below:
Privacy Risk: The sharing of data is necessary for individuals to receive benefits at the *Area Ann Arbor*. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: Safeguards implemented to ensure data is not shared inappropriately with organizations are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know purposes, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption and access authorization are all measures that are utilized within the administrations. Standing letters

for information exchange, business associate agreements and memorandums of understanding between agencies and VA are monitored closely by the Privacy Officer (PO), ISSO to ensure protection of information.

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

Section 6. Notice

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

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

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

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

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

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

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

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	Applicable SORs
VHA	• Non-VA Fee Basis Records-VA, SOR 23VA10NB3 • Patient Medical Records-VA, SOR 24VA10A7

Site Type: VBA/VHA/NCA or Program Office	Applicable SORs
	• Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA10 • 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 89VA10 • 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 121VA10 • Enrollment and Eligibility Records- VA 147-VA10NF1VHA Corporate Data Warehouse- VA 172VA10 • Health Information Exchange - VA 168VA005
NCPS	• 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 • Health Care Provider Credentialing and Privileging Records- VA¸SOR77VA10E2E • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10 • Income Verification Records-VA, SOR 89VA10 • Automated Safety Incident Surveillance and Tracking System- VA,SOR99VA13 • The Revenue Program Billings and Collection Records-VA, SOR114VA10 • National Patient Databases-VA, SOR 121VA10 • Enrollment and Eligibility Records- VA 147-VA10NF1VHA Corporate Data Warehouse- VA 172VA10 • Health Information Exchange - VA 168VA005

This Privacy Impact Assessment (PIA) also serves as notice of the Area Ann Arbor. 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.

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

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

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

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

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

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with Area Ann Arbor.

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

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

Information Consent Rights Table

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

Site Type: VBA VHA, NCA or Program Office	Information Consent Rights
	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 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that veterans and other members of the public will not know that the Area Ann Arbo*r* exists or that it collects, maintains, and/or disseminates PII, PHI or PII/PHI about them.
Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for health care. s. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SOR) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

Section 7. Access, Redress, and Correction

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

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

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this

section in addition to the agency's procedures. See 5 CFR 294 and the <u>VA FOIA Web page</u> to obtain information about FOIA points of contact and information about agency FOIA processes.

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

If the facilities within the Area are not a Privacy Act Area, 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 <u>VA Form 10-5345a: *Individuals' Request for a Copy of their Own Health Information*</u>, 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 <u>Healt*he*Vet program</u>, VA's online personal health record. More information about my Healt*he*Vet is available at <u>https://www.myhealth.va.gov/index.html</u>.

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

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

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

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

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that

even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.

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

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

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

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

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

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

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

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

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

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

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

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

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

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

Mitigation: Area Ann Arbor 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 Area Ann Arbor 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 Area, and are they documented?

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

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

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

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

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

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

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

Access to the Area Ann Arbor 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), through [*method of notice (email, fax 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 Area and the PII? If yes, what involvement will contractors have with the design and maintenance of the Area? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the Area?

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

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

Contractors will have access to the Area after completing the VA Privacy and Information Security Awareness training and Rules of Behavior annually, and after the initiation of a background investigation. Contractors are only allowed access for the duration of the contract this is reviewed by the privacy officer and the designated Contracting Officer Representative (COR). Per the National Contractor Access Program (NCAP) guidelines, contractors can have access to the Area only after completing mandatory information security and privacy training, Privacy and HIPAA Focused Training as well as having completed a Special Agency Check, finger printing and having the appropriate background investigation scheduled with Office of Personnel Management. Certification that this training has been completed by all contractors must be provided to the employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy. Contractors with VA Area Ann Arbor 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 Area?

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

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

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

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

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

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

8.4a If Yes, provide:

1. *The Systems Security Plan Status: Approved*
2. *The Systems Security Plan Status Date: 04/03/2023*
3. *The Authorization Status: Authorization to Operate (ATO)*
4. *The Authorization Date: June 16, 2023*
5. *The Authorization Termination Date: June 15, 2026*
6. *The Risk Review Completion Date: July 24, 2019*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): Moderate*

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

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

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

_____

Privacy Officer, Verona Robinson

_____

Assistant Privacy Officer, Malinda Williams

_____

Information System Security Officer, David Jones

_____

Area Manager, John Kucans

_____

APPENDIX A – Notice

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

Applicable Notices

Site Type: VBA/VHA/NCA or Program Office	*Applicable NOPPs*
VHA	**Notice of Privacy Practices** **VHA Privacy and Release of Information:**
NCPS	**Notice of Privacy Practices** **VHA Privacy and Release of Information:**

APPENDIX B – PII Mapped to Components

The completion of this section of the PIA will be in coordination with the Area Manager, Privacy Officer and ISSO. They may need to coordinate with the system (server/database) point of contact. This information must match the servers/databases listed in 3.5 of the Area PTA.

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

PII Mapping of Components (Servers/Database)

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNAPPCHKPT	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPDSG1	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
						restricted access controls	
VHAANNAPPSCRUBX	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNFONRESRAS	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNFONRESRGS	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNFONRESRR1	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNFONRESRS2	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
OITANNAPPSTRM01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
OITANNDHCW01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
OITANNHSMSFFX01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
OITANNSQLUNIFY	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
R03ANNCAVMS01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to	Advanced Encryption Standard (AES) 256, Server is	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
					facilitate patient care	stored in a secured environment and managed with restricted access controls	
R03ANNCAVMS02	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
R03ANNCAVMS03	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPP01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
						restricted access controls	
VHAANNAPPAPRONV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPCOSSAS	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPHCARTV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNAPPHSRD1	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPHSRD2	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPHSRD3	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPIMED	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to	Advanced Encryption Standard (AES) 256, Server is	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
					facilitate patient care	stored in a secured environment and managed with restricted access controls	
VHAANNAPPMDE01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPMMETER	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPQMATV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
						environment and managed with restricted access controls	
VHAANNAPPSCAN01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPVCM01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPVCM02	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNAPPVENV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNDFS1	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNEMRGCY1	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNLOGSPLNKV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
						managed with restricted access controls	
R03ANNCAVMS01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
R03ANNCAVMS02	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
R03ANNCAVMS03	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNAPP01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPAPRONV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPCOSSAS	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPHCARTV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
						managed with restricted access controls	
VHAANNAPPHSRD1	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPHSRD2	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPHSRD3	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNAPPIMED	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPMDE01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPMMETER	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPQMATV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
						managed with restricted access controls	
VHAANNAPPSCAN01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPVCM01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPP01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNAPPAPRONV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPCOSSAS	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPHCARTV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPHSRD1	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
						managed with restricted access controls	
VHAANNAPPHSRD2	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPHSRD3	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPIMED	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNAPPMDE01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPMMETER	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPQMATV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPSCAN01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
						managed with restricted access controls	
VHAANNAPPVCM01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPVCM02	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPVENV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNDFS1	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNEMRGCY1	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNLOGSPLNKV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNMONWUGV	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
						managed with restricted access controls	
VHAANNAPPAVA1	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPCERE02	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPDIFA	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNAPPDIHI	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPDIPRO	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPDIRPT	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPDITST	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
						managed with restricted access controls	
VHAANNAPPKEY01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPMINFO	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPPANDOR	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNAPPPOAN	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPPOP	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPPOT	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPRCP02	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
						managed with restricted access controls	
VHAANNAPPVELCTY	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPVISTA	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNAPPVOC02	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNFAXSTRM1	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNFAXSTRM3	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNFON01UM	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNFONOW5000	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
						managed with restricted access controls	
VHAANNFONVOCER2	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNFONVOCER3	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNFONVOCER4	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNFONVOCER5	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNFONVOCER6	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNPRT01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNPRT02	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
						managed with restricted access controls	
VHAANNPRTBIOPT	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNRTLBS1	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA
VHAANNWEB01	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

Components of the Area 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 Area (VBA, VHA, NCA, Program Office)
VHAANNAPPPOLY	Yes	Yes	Yes	Social Security Number, DOB	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls	VHA

APPENDIX C – List of Special Purpose Systems

This table is only to be completed for Special Purpose Systems. This information must match the special purpose systems listed in 3.7 of the Area PTA.

Name of Special Purpose Systems