Date PIA submitted for review:

3/10/2022

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

Area Louisville

Southeast District

Facilities Supported by the Area

Facilities Supported by the Area:
1. 1) Robley Rex VA Medical Center (VHA)
2. 2) Veterans Benefit Administration (VBA) Regional Office
3. 3) National Cemetery Administration (NCA)
4. 4) Zachary Taylor National Cemetery
5. 5) Fort Knox Community-Based Outpatient Clinic (CBOC)

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

6. 6) Carrollton CBOC
7. 7) Scottsburg CBOC
8. 8) Grayson CBOC
9. 9) New Albany CBOC
10.10) Shively CBOC
11.11) Stonybrook CBOC
12.12) Newburg CBOC
13.13) Greenwood CBOC
14.14) University of Louisville Off-site Radiology Reading Location
15.15) Louisville Veterans Center

Area Boundary Contacts:

Area Privacy Officer

Name	**Phone Number**	**Email Address**	**Location**
Alexander I. Slosman	502 287-5419	Alexander.Slosman@va.gov	Louisville, Kentucky VAMC
Michael Glock	502.566.4433	Michael.Glock@va.gov	VBA
Ginger Wilson	202 568-1260	Ginger.Wilson@va.gov	NCA

Area Information System Security Officer

Name	**Phone Number**	**Email Address**	**Location**
Joshua "Josh" Mulholland	859 233-4511	joshua.mulholland@va.gov	Lexington, Kentucky
Todd Finney	502 566-4507	Todd.Finney@va.gov	Louisville, Kentucky

Area Manager

Name	Phone Number	Email Address	Location
Augustine "Gus" Bittner	502 287-6977	Augustine.Bittner@va.gov	Louisville, Kentucky

Abstract

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

Louisville is an Information Area Boundary that consists of the Robley Rex VA Medical Center (VHA), Veterans Benefit Administration (VBA) Regional Office, National Cemetery Administration, Zachary Taylor National Cemetery, Fort Knox Community-Based Outpatient Clinic (CBOC), Carrollton CBOC, Scottsburg CBOC, Grayson CBOC, New Albany CBOC, Shively CBOC, Stonybrook CBOC, Newburg CBOC, Greenwood CBOC, University of Louisville offsite Radiology Reading Location, Louisville Veterans Center, Veterans Readiness and Employment Center in Bowling Green, Kentucky. The Area Boundary environment consists of components such as workstations, laptops, portable computing devices, terminals, servers, printers, and IT enabled networked medical devices that are owned, managed, and maintained by the facilities. The Area provides operational connectivity services necessary to enable users' access to information technology resources throughout the enterprise including those within the facility, between facilities, resources hosted at data centers, and connectivity to other systems. Network connectivity rules are enforced by VA approved baselines for router and switch configurations. The Area Boundary system environment also includes as applicable, subsystem storage utilities such as tape drives, optical drives, disk drives, network area storage (NAS), storage access networks (SAN), archival appliances, special purpose systems, and tier 2 storage solutions. The Area Boundary encompasses the management, operational, and technical security controls associated with IT hardware, consisting of servers, routers, switches, hubs, gateways, peripheral devices, desktop/laptops, and OS software. The Area Boundary employs a myriad of routers and switches that connect to the VA network.

Overview

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

- *The IT Area Boundary name and the name of the sites within it.*
- *The business purpose of the Area Boundary and how it relates to the program office and agency mission.*
- *Whether the Area Boundary is leveraging or accessing Enterprise repositories such as Veterans Benefits Management System, SharePoint, VistA, etc. and if so, a description of what PII/PHI from the Enterprise repositories is being used by the facilities in the Area Boundary.*

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

[Please pay attention to the bulleted questions above and make sure each question is addressed in the Overview response.]

The Louisville Area Boundary itself does not collect, use, disseminate, maintain, or store PII/PHI. VHA, VBA and NCA Facilities located within the Louisville BoundryIT Boundary all access VA Enterprise IT systems respectively, hosted and maintained outside of this boundary. These are VISTA, VBMS, MEM, etc.

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

The facilities within the Area IT Boundary collect, use, and/or disseminate PII/PHI that is maintained and stored within enterprise systems such as VistA, VBMS, BOSS/AMASS, etc. There are individual PIAs that contain detailed information on the maintenance, dissemination and sharing practices, and storage of the PII/PHI for each Enterprise system accessed by the facilities.

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

The applicable SORs for Louisville 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 • Patient Medical Records-VA, SOR 24VA10A7 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA10 • Community Placement Program-VA, SOR 65VA122 • Health Care Provider Credentialing and Privileging Records-VA¸SOR 77VA10E2E • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10 • Income Verification Records-VA, SOR 89VA10NB

Site Type: VBA/VHA/NCA or Program Office	*Applicable System of Records (SORs)*
	• Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA13 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10 • National Patient Databases-VA, SOR 121VA10A7 • Enrollment and Eligibility Records- VA 147VA10NF1 • VHA Corporate Data Warehouse- VA 172VA10A7 • Health Information Exchange - VA 168VA005
VBA	• Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28
NCA	• Veterans and Dependents National Cemetery Gravesite Reservation Records - VA SOR 41VA41 • Veterans and Dependents National Cemetery Interment Records - VA SOR 42VA41 • Veterans (Deceased) Headstone or Marker Records - VA, SOR 48VA40B • VA National Cemetery Pre-Need Eligibility Determination Records - VA SOR 175VA41A

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Tax Identification Number
☒ Medical Record Number
☒ Next of Kin
☒ Guardian Information
☒ Electronic Protected Health Information (ePHI)
☒Military History/Service Connection
☒Service-connected Disabilities
☒Employment Information
☒ Veteran Dependent Information
☒ Disclosure Requestor Information
☒ Death Certification Information
☒ Criminal Background
☒ Education Information
☒ Gender
☒ Tumor PHI Statistics
☐ Other Unique Identifying Information (list below)

PII Mapping of Components

Louisville Area Boundary consists of 26 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 Louisville Area Boundary and the reasons for the collection of the PII are in the **Mapping of Components Table in Appendix B of this PIA.**

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

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

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

The information collected, maintained, and/or disseminated by Louisville Area comes from a variety of sources. Depending on the type of information, it may come directly from the Veteran

or patient, from programs and resources in the Veterans Benefits Administration (VBA), the VA Health Eligibility Center (HEC), Department of Defense (DoD), VA Network Authorization Office (NAO) for non-VA Care payments, and non-VA medical providers.

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

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

Additional sources include:

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

1.3 How is the information collected?

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

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

The information is collected directly from patients, employees, and/or others using paper forms, online data entry on encrypted information systems (i.e. Enrollment form for VA Health Care), or interviews and assessments with the individual. Information from outside sources is collected

in several ways, including encrypted transmission and receipt from multiple outside agencies (i.e. DoD, OGC, etc.)

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.
VBA	There are many VA forms used by Veterans to apply for and/or make adjustments to pending benefits. All VBA benefit forms are located at http://www.va.gov/vaforms/. The URL of the associated privacy statement is: http://www.va.gov/privacy/. VBA forms can be downloaded from this site, filled in and printed to be delivered in paper form. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury. The VBA toll free number for veterans is 1-800-827-1000. Clients are referred to and transferred to the Regional Office of Jurisdiction, where they can provide a service representative with required information. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury. VBA employees may also contact a Veteran directly to obtain clarifying information for a claim for benefits.
NCA	MEM does not receive information electronically from other systems. Information is collected through direct phone calls to the NCSO or A long-term plan is in place for the Pre-Need system to transmit data electronically to the EOAS component of BOSS, but these activities are currently processed by scheduling office personnel. Documents from funeral homes, next of kin, and other points of contact from the decedent are sent to scheduling office personnel and uploaded into BOSS. AMAS processes approximately 360,000 claims for standard government headstones or markers (VA Form 40-1330) and

Site Type: VBA/VHA/NCA or Program Office	*Means of Collection*
	Monument and Presidential Memorial Certificate Request (VA Form 40-0247) applications annually. Data from the forms are manually entered into the system. Forms and supporting documentation required to verify memorial benefits eligibility, such as the DD214, are scanned/uploaded.

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.

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

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

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

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

10. Employee and VA contractor information is maintained based on Human Resources (HR) and payroll needs and Federal contracting requirements.

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

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

Purpose of Information Collection Table

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

Site Type: VBA/VHA/NCA or Program Office	*Purpose of Information Collection*
NCA	• MEM collects and maintains information to verify the identity and eligibility of the Veteran or decedent for burial and monument services

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

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

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

Information obtained directly from the individual will be assumed to be accurate. Information may be verified with other Federal agencies (VBA, DOD, SSA and IRS) to confirm eligibility or benefits. Should conflicting information come to the attention of facility staff, it will be documented and verified prior to further use.

Furthermore, individuals have the right to obtain access to their records and request correction to them when necessary. Patient demographic as well as income verification matching completed by automated tools with connections to the Austin Automation Center are obtained. Practitioners review and sign all treatment information and Health Information Management Service reviews data obtained and assists with corrections.

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

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

List the full legal authority for operating the Area Boundary, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in

addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.

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

Louisville Area is a facility level entity that operates under the authority of Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a). Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:

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). • **Freedom of Information Act (FOIA),** 5 USC 552. • **Privacy & Release of Information,** VHA Directive 1605.01. • **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**, Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules). • **Health Information Technology for Economic and Clinical Health (HITECH) Act,** Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq. • **Privacy Act of 1974,** 5 U.S.C. 552a • **Federal Information Processing Standards (FIPS) 140-2,** approved encryption algorithms and products • **Federal Information Processing Standards Publication (FIPS PUB) 199,** Standards for Security Categorization of Federal Information and Information Systems Version Date: February 27, 2020 • **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47,** Security Guide for Interconnecting • **National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 60,** Guide for Mapping Types of Information and Information Systems to Security Categories.

	• **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53,** Rev. 4, Recommended Security Controls for Federal Information Systems • **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88,** Guidelines for Media Sanitization • **Trade Secrets Act** (18 U.S. Code 1905) • **Unauthorized Access Act** (18 U.S. Code 2701 and 2710) • **VA Directive 6371,** Destruction of Temporary Paper Records • **VA Directive 6600,** Responsibility of Employees and Others Supporting VA in Protecting Personally Identifiable Information (PII) • **VA Directive and Handbook 6500,** Information Security Program • **VA Directive and Handbook 0710,** Personnel Suitability and Security Program
VBA	• Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b)
NCA	• Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(a), 501(b), and Chapter 24, Sections 2400-2404.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

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

Privacy Risk:
The Louisville Area collects both 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:

The Louisville Area deploys extensive security measures, in a defense in depth framework, 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. Our facility 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 National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

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

Section 2. Uses of the Information

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

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

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

Due to the extensive amount and nature of the information contained in the Louisville Area General Support System, maintained by the Southeast District GSS, it is impossible to independently list each data point collected and describe its purpose. Below is a description of how different categories of data are used. If you have questions about a certain data point, please contact your facility privacy officer to learn more.

- **Name**: Used to identify the patient during appointments and patients and employees in other forms of communication.
- **Social Security Number**: Used as a patient and employee identifier and as a resource for verifying income information with the Social Security Administration.
- **Date of Birth**: Used to identify age and confirm patient identity.
- **Mother's Maiden Name**: Used to confirm patient identity.
- **Mailing Address**: Used for communication, billing purposes and calculate travel pay.
- **Zip Code**: Used for communication, billing purposes and calculate travel pay.
- **Phone Number(s)**: Used for communication, confirmation of appointments and conduct tele health appointments.
- **Fax Number**: Used to send forms of communication and records to business contacts, insurance companies and health care providers.
- **Email Address**: Used for MyHealtheVet secure communications.
- **Emergency Contact Information (Name, Phone Number, etc. of a different individual)**: Used in cases of emergent situations such as medical emergencies.
- **Financial Account Information**: Used to calculate co-payments and VA health care benefit eligibility.
- **Health Insurance Beneficiary Account Numbers**: Used to communicate and bill third party 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 Numbe**r: Used to track vehicles on VA grounds by VA Police to quickly identify vehicle ownership and authorization to be on facility grounds.
- **Internet Protocol (IP) Address Numbers**: Used to track, identify and locate a device on a network and to ensure no two devices are assigned the same IP.
- **Gender**: Used for patient demographic information.
- **Previous Medical Records**: Used for continuity of health care.
- **Current Medications**: Used within the medical records for health care/treatment purposes.
- **Race/Ethnicity**: Used for patient demographic information and for indicators of ethnicity-related diseases.
- **Next of Kin**: Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
- **Guardian Information**: Used when a representative has been appointed or designated because the patient is unable to make decisions.
- **Electronic Protected Health Information (ePHI):** Used for history of health care treatment, during treatment and plan of treatment when necessary.

- **Military history/service connection**: Used to evaluate medical conditions that could be related to location of military time served. Also used to determine VA benefit and health care eligibility.
- **Service-connected disabilities**: Used to determine VA health care eligibility and treatment plans/programs.
- **Employment information**: Used to determine VA employment eligibility and for Veteran contact, financial verification.
- **Veteran dependent information**: Used to determine benefit support and as an emergency contact person.
- **Disclosure requestor information**: Used to track and account for patient medical records released to requestors.
- **Education information**: Used to determine VA employment eligibility as well as for patient health care/treatment purposes.
- **Medical statistics**: Used for research purposes containing PII/PHI.
- **Date of Death**: Used for death certificate, benefits and memorial honors.
- **Criminal background**: Used to determine VA employment eligibility as well as patient health care/treatment purposes.
- **Tumor PII/PHI Statistics**: Used to evaluate medical conditions and determine treatment plan

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

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

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

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

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

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

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

These reports may track:

- Reports created to analyze statistical analysis on case mixes.
- Analyze the number of places and geographical locations where patients are seen to assess the volume
- of clinical need.
- Analyze appointment time-frame data to track and trend averages of time. 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.
- Patient specific orders
- Unique patient trends
- Clinic wait times

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

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

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 HIPAA training; face-to-face training for all incoming employees conducted by the Information Security Officer and Privacy Officer; regular audits of individuals accessing sensitive information; and formal rounds during which personal examination of all areas within the facility to ensure information is being appropriately used and controlled.

Section 3. Retention of Information

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

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

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

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

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

- Name
- Social Security Number
- Date of Birth
- Mother's Maiden Name
- Mailing Address
- Zip Code
- Phone Number(s)
- Fax Number
- Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information

- Health Insurance Beneficiary Numbers
- Account Numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Gender as provided by the patientName and contact information for Guardian as provided by the patient
- Military and service history as provided by the patient and/or VBA
- Employment information as provided by the patient
- Veteran dependent information as provided by the patient
- Education information as provided by the patient
- Name and contact information for Next of Kin
- Service-Connected rating and disabilities (based on information provided by Veteran and/or VBA)
- Date of death as supplied by Next of Kin or provider
- Criminal background and dependent information as reported by patient and/or national databases
- ePHI
- Next of Kin
- Gaurdian Information
- Tumor PII/PHI statistics
- Veteran dependent information
- Disclosure requestor information
- Service Connected disabilities

3.2 How long is information retained by the facilities?

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

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

The Louisville Area follows the guidelines established in the Department of Veterans Affairs, Veterans Health Administration Record Control Schedule (RCS) 10-1, Part Three, Chapter Six, Code 6000.2(b) (May 2016), which mandates patient health records are retained for 75 years after the last episode of medical care

Length of Retention Table

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

Site Type: VBA/VHA/NCA or Program Office	*Length of Retention*
	entitlement or upon the exceeding of a Veteran's delimiting date of eligibility (generally, ten or twelve years from discharge or release from active duty), whichever occurs first, and then destroyed. • Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA. • Education electronic folders are retained at the servicing Regional Processing Office. Education folders may be destroyed in accordance with the times set forth in the Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA. • Employee productivity records are maintained for two years after which they are destroyed by shredding.
NCA	• Veterans (Deceased) Headstone or Marker Records-VA SORN 48VA40B: Retained indefinitely

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

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

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

Retention Schedule Table

Site Type: VBA/VHA/NCA or Program Office	*Retention Schedule*
VHA	When managing and maintaining VHA data and records, Louisville Area follows the guidelines established in the NARA-approved Department

Site Type: VBA/VHA/NCA or Program Office	*Retention Schedule*
	of Veterans' Affairs Record Control Schedule (RCS)-10 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf); Department of Veterans Affairs, Office of Information & Technology RCS 005-1(http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf) and the General Records Schedule (http://www.archives.gov/records-mgmt/grs/).
VBA	When managing and maintaining VBA data and records, Louisville Area follows the guidelines established in the NARA-approved Records Control Schedule VB-1, Part I, FieldVeterans Benefits-1
NCA	When managing and maintaining VBA data and records, Louisville Area follows the guidelines established in Veterans (Deceased) Headstone or Marker Records-VA, SOR 48VA40B.

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

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

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

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8310

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the **Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization** (November 3, 2008), http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=416&FType=2.

When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1.
Additionally, Louisville Area follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents **as well as** FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

3.5 Does the Area Boundary include any facility or program that, where feasible, uses techniques to minimize the risk to privacy by using PII for research, testing, or training?
Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

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

No PII or PHI is used to test systems prior to deployment, and all testing or training is conducted using test samples of fabricated data. The Louisville Area research department adheres to the guidelines established in VA Record Control Schedule (RCS)-10 and VA Record Control Schedule (RCS) 005-1.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

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

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

Mitigation:

In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed in GSS is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary. To mitigate the risk posed by information retention, Louisville Area 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 Louisville Area ensures that all personnel involved with the collection, use and retention of data are trained in the correct process for collecting, using and retaining this data. A Records Management Officer (RMO), Privacy Officer (PO) and an Information System Security Officer (ISSO) are assigned to the facility to ensure their respective programs are understood and followed by all to protect sensitive information form the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning the proper handling of 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 Boundary sharing/receiving/transmitting information with? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

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

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

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

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

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

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

List the Program 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***	***Provide name of Applicable Area Sites***
Veterans Benefits Administration	Examinations and eligibility for VA benefits	Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	Compensation and Pension Record Interchange (CAPRI) electronic software package	Area Louisville
National Cemetery Administration	Verification of Death Benefits	Pertinent PII, PHI, and III appropriate to the request Service dates, SSN, demographics, service connection, military records	Transmitted upon request in an electronic, written, or verbal format based on the individual request	Area Louisville
VA Veteran Centers	Community of Care, eligibility, and enrollment	Pertinent PII, PHI, and III appropriate to the request Service dates, SSN, demographics, service connection, military records	Accessible by Vet Center staff via CPRS	Area Louisville
Health Eligibility Center	Healthcare eligibility information	Service dates, SSN, demographics, service connection	Scanned documents uploaded into shared software program.	Area Louisville
Austin Automation Center	Healthcare encounter information	Name, date of birth, Sex, SSN, demographics and health information	Information may be transmitted electronically. AAC employees can log into CPRS or VistA.	Area Louisville

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***	***Provide name of Applicable Area Sites***
VHA programs or contracts with a business need to know	Access for assistance with the Wounded Warrior Project	Pertinent PII, PHI, and III appropriate to the request Service dates, SSN, demographics, service connection, military records	Transmitted upon request in an electronic, written, or verbal format based on the individual request.	Area Louisville
National Veteran's Service Organization – specific organization such as Veterans of Foreign WAR (VFW), etc.	Helps members apply for VA benefits	Pertinent PII, PHI, and III appropriate to the request Service dates, SSN, demographics, service connection, military records	Transmitted upon request in an electronic, written or verbal format based on the individual request.	Area Louisville
Department of Veterans Affairs General Counsel Office	Information supporting litigation for pending cases.	Pertinent PII, PHI, and III appropriate to the request Service dates, SSN, demographics, service connection, military records	Transmitted upon request in an electronic, written or verbal format based on the individual request.	Area Louisville
VA Network Authorized Office Non-VA Care	Health/medical payment authorization	Pertinent PII, PHI, and III appropriate to the request Service dates, SSN, demographics,	Fee Basis Claim system (FBCS) authorization software program	Area Louisville
Data Services	Healthcare encounter information	Pertinent PII, PHI, and III appropriate to the request Service dates, SSN, demographics, service connection, military records	Electronically via VistA through Computerized Patient Record System (CPRS)	Area Louisville
VA Network Authorized Office	Health/medical payment authorization	Pertinent PII, PHI, and III appropriate to the request Service dates,	HTTPS using SSL encryption	Area Louisville

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*	*Provide name of Applicable Area Sites*
Non-VA Care Payments		SSN, demographics, service connection, military records	and certification exchange fee	
Consolidated Patient Account Center	Health/medical payment authorization	Pertinent PII, PHI, and III appropriate to the request Service dates, SSN, demographics, service connection, military records	VistA Direct Access	Area Louisville
VA Network Authorized Office Non-VA Care Payments	Health/medical payment authorization	Pertinent PII, PHI, and III appropriate to the request Service dates, SSN, demographics, service connection, military records	HTTPS using SSL encryption and certification exchange fee	Area Louisville
Internal Secure SharePoint Portal	To securely exchange multiple PHI/PII/VASI data sets	Pertinent PII, PHI, and III appropriate to the request Service dates, SSN, demographics, service connection, military records	Information transmitted electronically over secure LAN connection	Area Louisville
Board of Veterans Appeals	To securely exchange PII to effect appeals by Veterans	Pertinent PII, PHI, and III appropriate to the request Service dates, SSN, demographics, service connection, military records.	Transmitted upon request in an electronic, written or verbal format based on the individual request	Area Louisville

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.

Privacy Risk:

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

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

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

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

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

Section 5. External Sharing/Receiving and Disclosure

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

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

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

Note: Question #3.6 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 an Area Boundary outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a

Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

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

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

Data Shared with External Organizations

List External Program Office or IT 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***	***List names of Applicable Area Sites***
S Abbott	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0530)	Robley Rex VA Medical Center
Alere	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0175/0250)	Robley Rex VA Medical Center (VHA) Reading Location
BEYER	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0355)	Robley Rex VA Medical
BioMerieux	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0540)	Robley Rex VA Medical Center
Extension	Remote support and system diagnostic.	System log files, sample clinical data	National MOU/ISA	S2S VPN (CID:0097)	Robley Rex VA Medical Center

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
		that may contain PHI/PII.			
GE Med-IT	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0166)	Robley Rex VA Medical Center
LabCorp	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0173)	Robley Rex VA Medical Center
McKesson	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0472)	Robley Rex VA Medical Center
Ortho-Clinical	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0511)	Robley Rex VA Medical Center
Philips	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0184)	Robley Rex VA Medical Center
Siemens	Remote support and system diagnostic.	System log files, sample clinical data that may	National MOU/ISA	S2S VPN (CID:0183)	Robley Rex VA Medical Center

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
		contain PHI/PII.			
Sorna	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0267)	Robley Rex VA Medical Center
SysMex	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0298)	Robley Rex VA Medical Center
TOPCON	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0164)	Robley Rex VA Medical Center
VENCA	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0333)	Robley Rex VA Medical Center
VetMedd	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	National MOU/ISA	S2S VPN (CID:0368)	Robley Rex VA Medical Center
Department of Defense (DOD)	Determine military service dates, Eligibility	Name, Date of Birth, Sex, SSN, demographics	SORN 24VA10P2, Routine use 1, National sharing	Information is uploaded/downloaded electronically to the database.	Robley Rex VA Medical Center

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
		and health information.	agreement, VA SORN 168VA10P2		Louisville Veteran's Center (VBA) Regional Office VRE Center (Bowling Green) National Cemetery Administration (NCA)
FOIAExpress	Legal/Regulatory	Pertinent PII, and III appropriate to the request including but not limited to name, demographics, as it relates to any VA record.	Legal authority and binding agreement	Information is uploaded electronically to the database.	Robley Rex VA Medical Center
Social Security Administration (SSA)	Eligibility for Federal benefits	Name, Date of Birth, Sex, SSN, demographics	Title 38, United States Code, Section 5701	Site to Site (S2S), IPSEC Tunnel, Secure FTP	Robley Rex VA Medical Center Veterans Benefit Administration (VBA) Regional Office National Cemetery

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*	*List names of Applicable Area Sites*
					Administration (NCA)
Office of Personnel Management (OPM)	Determine military and civilian service dates, employment eligibility	Pertinent Personally Identifiable Information (PII) and Individually Identifiable Information (III). Name, DOB, demographics, SSN, all employee HR records.	National ISA/MOU	Information is uploaded/downloaded to/from electronic database.	Robley Rex VA Medical Center
Federal Emergency Management Agency (FEMA)	Eligibility for Federal benefits	First and last name, SSN, dob	Homeland Security Presidential Directive – 5 requires all federal agencies to comply as required with FEMA directives during emergencies.	Information may be transmitted upon request in an electronic, written, or verbal format based on the individual requests.	Robley Rex VA Medical Center
Federal Bureau of Investigation	Determine eligibility based on current and/or background criminal information	PHI and PII, Name, SSN, DOB, Address	VA SORN 2VA135 VA SORN 79VA19	Electronic VA FBI website	Robley Rex VA Medical Center
Kentucky Cabinet for Health and Family Services	Health information regarding	PHI and PII, Name, SSN, DOB, Address	900, 901, 902 –CH. 2, 906, and 922	Via secure portal and/or secure fax	Robley Rex VA Medical Center

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
	infectious diseases.		Kentucky Administrative Regulations and Kentucky Revised Statutes 218A.202; Title 38, United States Code, Section 5701; VHA Standing Letter agreement; SORN 24VA10P2		
State of Kentucky Vital Statistics Office	Health information in	PHI and PII, Name, SSN, DOB,	901 KAR; Title 28, United States Code, Section 5701	Via secure portal and/or secure fax	Robley Rex VA Medical Center
Internal Revenue Service	Demographic and income verification to determine eligibility for medical benefits	PHI and PII, Name, SSN, DOB, Address	SORN 89 VBA10NB, Income Verification Records- VA; Privacy Act of 1874, 5 United States Code 552a(e), Public Law 101-508 Omnibus Budged Reconciliation Act of 1990	Via secure portal and/or secure fax	Robley Rex VA Medical Center

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT System***	***List the specific data element types such as PII/PHI that are shared/received with the Program or IT System***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***	***List names of Applicable Area Sites***
State Prescription Management Program	Monitor and manage prescription of control medication	PHI and PII, Name, SSN, DOB, Address	Data Use Agreement	Secure FTP	Robley Rex VA Medical Center
Endicia	Postage Metering and accounting information	PII	MOU/ISA	HTTPS/Secure FTP	Robley Rex VA Medical Center
AcuStaf	Manage and control clinical staff schedule assignments	PII	MOU/ISA	S2S	Robley Rex VA Medical Center
Arixum	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	MOU/ISA	S2s	Robley Rex VA Medical Center
Fire Alarm Monitoring	Remote support and system diagnostic.	System log files, sample clinical data that may contain PII.	MOU/ISA	Secure FTP	Robley Rex VA Medical Center
Hill Rom	Remote support and system diagnostic.	System log files, sample clinical data that may contain PII.	MOU/ISA	S2S	Robley Rex VA Medical Center
Lenel	Remote support and system diagnostic.	System log files, sample clinical data that may contain PII.	MOU/ISA	S2s	Robley Rex VA Medical Center
Medivator	Remote support and system diagnostic.	System log files, sample clinical data	MOU/ISA	S2s	Robley Rex VA Medical Center

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*List names of Applicable Area Sites*
		that may contain PII.			
Roche	Remote support and system diagnostic.	System log files, sample clinical data that may contain PHI/PII.	MOU/ISA	S2S	Robley Rex VA Medical Center
Snyder Engineering	Remote support and system diagnostic.	No PHI/PII	MOU/ISA	S2S	Robley Rex VA Medical Center
University of Louisville	Veteran PHI/PII used by researchers and providers for community-based care recipients	PHI and PII, Name, SSN, DOB, Address	MOU/ISA	S2S	Robley Rex VA Medical Center
UPS World Ship	Postage Metering and accounting information	PII	MOU/ISA	S2S	Robley Rex VA Medical Center
Venca	PII used to track demographics of Veteran healthcare data	PII	MOU/ISA	S2S	Robley Rex VA Medical Center

The following measures have been taken to meet the requirements of OMB Memoranda M-06-15, dated 05/22/06:

- Louisville Area requires all employees complete mandatory 10176 training, that includes agreeing to a specific set of Rules of Behavior based on their status as an "organizational user" or "non-organization user." The Rules of Behavior are set forth in VHA Handbook 6500, Appendix D.
- Louisville Area has established appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity, which could result in substantial harm,

embarrassment, inconvenience or unfairness to any individual whom information is maintained as follows:

- Louisville Area has long-standing requirements involving mandatory training prior to accessing records, annual training that stresses confidentiality and safeguarding information, quarterly audits that ensure compliance, assignment of Functional Category for each employee that defines the minimum necessary access that is needed for their official job duties, encryption is utilized by staff when PHI/PII is emailed internally and externally, PIV cards have been implemented, according to Homeland Security Presidential Directive (HSPD-12) guidance.
- Louisville Area conducts continuous monitoring of all security and privacy controls in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53 and is compliant with the Federal Information Security Management Act (FISMA).
- Louisville Area reviews all facility policies to ensure adequate safeguards are in place for their processes to prevent the intentional, negligent misuse of, or unauthorized access to personally identifiable information. All new and updated facility policies are routed for Privacy Officer's concurrence prior to Director's signature. A list of all policies and privacy elements are maintained on a spreadsheet by Privacy Officer.
- Louisville Area reports privacy and security incidents to the VA Cyber Security Operations Center (CSOC) within one hour of discovery and anything that is of a criminal nature or needs to be reported to authorities outside the VA is promptly and completely reported to the proper authorities, including Inspectors General and other law enforcement authorities. In certain circumstances, this reporting also includes the Department of Homeland Security (DHS).

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

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

Privacy Risk:

The sharing of data is necessary for the medical care of individuals eligible to receive care in Louisville Area. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation:

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

All personnel accessing Veteran's information must first have a successfully adjudicated background screening (SAC). This background check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history records. A background investigation is required commensurate with the individual's duties.

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

Section 6. Notice

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

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

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

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

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

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

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A signed statement acknowledging that the individual read and understood the NOPP is scanned into each

applicant's electronic file. When updates are made to the NOPP copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.

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

The Department of Veterans Affairs provides additional notice of this system by publishing 2 System of Record Notices (SORNs):

1. The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Feb. 11, 2014), in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2014-08-14/pdf/2014-19283.pdf
2. The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10P2 (Amended Oct. 31, 2012), in the Federal Register and online. An online copy of the SORN can be found at: https://www.oprm.va.gov/docs/sorn/SORN79VA10P2.PDF

The following VA System of Record Notices (SORNs) also apply:

Applicable SORs

Site Type: VBA/VHA/NCA or Program Office	***Applicable SORs*** .
VHA	• Individuals Serving on a Fee Basis or Without Compensation (Consultants, Attending's, and Others or Paid Indirectly through a Disbursement Agreement) Personnel Records-VA, SORN 14VA05135 • Non-VA Fee Basis Records-VA, SORN 23VA163 • Patient Medical Records-VA, SORN 24VA19 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SORN 34VA12 • Community Placement Program-VA, SORN 65VA122 • Health Care Provider Credentialing and Privileging Records-VA¸SORN 77VA10Q • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SORN 79VA10P2 • Income Verification Records-VA, SORN 89VA19

Site Type: VBA/VHA/NCA or Program Office	*Applicable SORs* .
	• Automated Safety Incident Surveillance and Tracking System-VA, SORN 99VA131 • Telephone Service for Clinical Care Records- VA, SORN 113VA112 • The Revenue Program Billings and Collection Records-VA, SORN 114VA16 • National Patient Databases-VA, SORN 121VA19
VBA	• Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SOR 58VA21/22/28
NCA	• Veterans and Dependents National Cemetery Gravesite Reservation Records -VA SOR 41VA41 • Veterans and Dependents National Cemetery Interment Records-VA SOR 42VA41 • Veterans (Deceased) Headstone or Marker Records-VA, SOR 48VA40B • VA National Cemetery Pre-Need Eligibility Determination Records - VA SOR 175VA41A

https://www.oprm.va.gov/privacy/systemsofrecords.aspx

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

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	Individuals may request in writing a record restriction limiting the use of their information by filling out a 10-5345 form. The request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to 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."
VBA	Once information is provided to VBA, the records are used, as necessary, to ensure the administration of statutory benefits to all eligible Veterans, Service members, reservists, and their spouses, surviving spouses and dependents. As such, individuals are not provided with the direct opportunity to consent to uses of information. However, if an individual wishes to remove consent for a particular use of their information, they should contact the nearest VA regional office, a list of which can be found on the VBA website.
NCA	Responding to collection is voluntary; therefore, consent of use is not applicable.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk:

There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and Louisville Area VAHCS prior to providing the information to the VHA.

Mitigation:
This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries and periodic monitoring is performed to check that the signed acknowledgment form has been scanned into electronic records. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SOR) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

Section 7. Access, Redress, and Correction

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

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

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

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

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

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

When requesting access to one's own records, patients are asked to complete VA Form 10-5345a: Individuals' Request for a Copy of their Own Health Information, which can beobtained from the medical center or online at http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf.

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

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

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

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

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

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

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

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

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

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

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

As discussed in question 6.1, the Notice of Privacy Practice (NOPP), which every patient signs prior to receiving treatment, discusses the process for requesting an amendment to one's records. Beneficiaries are reminded of this information when the NOPP is mailed to them by VA Privacy Office and humanitarians receive a copy of NOPP and signs prior to receiving treatment. Veterans are informed of the amendment process by many resources to include the Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information.
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

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

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

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

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

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

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

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

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

Mitigation:
Area Louisville 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 Notice of Privacy Practice (NOPP), which every patient must sign prior to receiving treatment, discusses the process for requesting an amendment to one's records. Beneficiaries are reminded of this information when the NOPP is mailed to them by VA Privacy Office.

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

The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll to obtain access to all the available features. In addition, Privacy Handbook 1605.1 establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

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

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

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

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

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

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

Human Resources notify Divisions, IT and ISSO of new hires and their start date(s), either through [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.

And "Individuals receive access to the Area Louisville 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 Louisville 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 to computer rooms at the Louisville Area facilities is limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Information that is downloaded from VistA and maintained on laptops and other approved government equipment is afforded similar storage and access protections as the data that is maintained in the original files. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at Louisville Area, or an OIG office location remote from Louisville Area, is controlled in the same manner.

Full time VARO employees, as their job requires it, have access to change Veteran Service Representative (VSR) and (RVSR) Rating Veteran Service Representatives have access to amend/change the information in the system, under the guidelines of least privilege, that is, users are granted the minimum accesses necessity to perform their duties. Work Study's' are limited to Inquiry only commands. Veteran Service Organizations (Co-located VSOs) and County or Out based VSOs (CVSOs) also have access to VA systems. These accesses are predefined and limited for these users. Individuals are subject to a background investigation before given access to Veteran's information. Private Attorneys, Claim Agents and Veteran Service Organizations Representatives must be accredited through the Office of General Counsel.

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

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

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

Each contract is reviewed prior to approval based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee). This review is conducted each time the contract period expires.

Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, signing the contractor Rules of Behavior, VHA HIPAA training as well as the appropriate background investigation to include fingerprinting. Certification that these items have all been completed by all contractors must be provided to the VHA employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a

Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy.

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

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

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

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

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*
8. *Has the Privacy Overlay been applied in eMASS?*

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

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

Yes

1. The Security Plan is Approved
2. The Security Plan Status Date, 10 – Dec -2021
3. The Authorization Status, Authorization to Operate (ATO)
4. The Authorization Date, 18-Feb-2022
5. The Authorization Termination Date, 18-Feb-2023

6. The Risk Review Completion Date, 14-Jan-2022
7. The FIPS 199 classification of the system is Moderate.
8. The Privacy Overlay has been applied in eMASS.

The Louisville Area (LOU-VHA) system was granted a full Authority to Operate on March 16, 2020 for one year. The Current FIPS 199 system classification is MODERATE.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Privacy Officers

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

ALEXANDER SLOSMAN Digitally signed by ALEXANDER SLOSMAN
Date: 2022.04.01 15:50:08 -04'00'

Privacy Officer, Alexander I. Slosman

MICHAEL GLOCK Digitally signed by MICHAEL GLOCK
Date: 2022.04.04 09:41:06 -04'00'

Privacy Officer, Michael Glock

Wilson, Ginger Digitally signed by Wilson, Ginger
Date: 2022.04.04 09:17:49 -05'00'

Privacy Officer, Ginger Wilson

Signature of Information System Security Officers

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

JOSHUA J. MULHOLLAND 3423844

Digitally signed by JOSHUA J. MULHOLLAND 3423844
Date: 2022.04.01 18:28:24 -04'00'

Information System Security Officer, Joshua Mulholland

Todd M Finney 1516592

Digitally signed by Todd M Finney 1516592
Date: 2022.04.04 08:27:59 -04'00'

Information System Security Officer, Todd Finney

Signature of Area Manager

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

AUGUSTINE BITTNER Digitally signed by AUGUSTINE BITTNER
Date: 2022.04.04 10:28:59 -04'00'

Area Manager, Augustine Bittner

APPENDIX A – Notice

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

Applicable Notices

Site Type: VBA/VHA/NCA or Program Office	***Applicable NOPPs***
VHA	**Notice of Privacy Practices** **VHA Privacy and Release of Information:**
^VBA	**Privacy Statement on VA Forms:** PRIVACY ACT INFORMATION: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA Programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is required to obtain or retain benefits. VA uses your SSN to identify your claim file. Providing your SSN will help ensure that your records are properly associated with your claim file. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by Federal Statute of law in effect prior to January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine maximum benefits under the law. The responses you submit are considered confidential (38 U.S.C. 5701). Information submitted is subject to verification through computer matching programs with other agencies **SOR 58VA21/22/28**
/NCA	**VA Form 40-0247** **VA Form 40-1330** **VA Form 40-1330M**

APPENDIX B – PII Mapped to Components

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

PII Mapped to Components Table

Components of the Area Boundary collecting/storing PII *(Each row refers to a grouping of databases associated with a single server)*	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Provide Names of Applicable Sites***
Server 1 • EMR (VistARO) • Lou_BioPoint_PI6 (Patient Wristbands) • MRS_LIVE (Mammography) NOAH - Audiology	Yes	Yes	Yes	Personally Identifiable Demographic Factors Including DOB and SSN, Contact Information, Health Information, Family History, Military/Veteran History and Status and Healthcare history	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	Robley Rex VA Medical Center
Server 2 AccuCheck – Glucometer	Yes	Yes	Yes	Personally Identifiable Demographic Factors Including	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server is stored in a secured	Robley Rex VA Medical Center

Components of the Area Boundary collecting/storing PII (*Each row refers to a grouping of databases associated with a single server****)***	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Provide Names of Applicable Sites***
				DOB and SSN, Contact Information, Health Information		environment and managed with restricted access controls	
Server 3 • BHL_LOU_PROD (Behavior Health Lab) • EncoreDB – CPAP • iMed 37 – EEG PandoraVIA – Pyxis Reporting System	Yes	Yes	Yes	Personally Identifiable Demographic Factors Including DOB and SSN, Contact Information, Health Information	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	Robley Rex VA Medical Center