Date PIA submitted for review:

January 13th, 2025

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

Area Columbia-
Missouri
Midwest District

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

Sites within Area:

Sites	*Station Numbers*
1) Harry S Truman VAMC, Columbia, MO	589A4
2) Waynesville CBOC	589A4
3) Jefferson City CBOC	589A4
4) Kirksville CBOC	589A4
5) Mexico CBOC	589A4
6) Sedalia CBOC	589A4
7) St. James CBOC	589A4
8) Marshfield CBOC	589A4
9) Camdenton CBOC	589A4
10) Buttonwood CBOC	589A4
11) Columbia Vet Center (CVC)	589A4

Area Contacts:

Area Key Stakeholders[2]

Name	*Title (PO, ISSO, AM)*	*Phone Number*	*Email Address*	*Applicable Site (VHA Program Office)*
Dorotheé C. Smith	Privacy Officer	573-814-6589	Dorothee.smith@va.gov	VHA-Harry S. Truman VAMC Columbia, MO
Julie VanSteenburgh	ISSO	573-228-8803	Julie.Vansteenburgh@va.gov	VHA-Harry S. Truman VAMC Columbia, MO
Jeffrey Simkins	Service Area Manager	573-814-6566	Jeffrey.Simkins@va.gov	VHA-Harry S. Truman VAMC Columbia, MO

Legend:

[2] NOTE: Readjustment Counseling Service (RCS) Privacy Officer must be listed as a stakeholder for review and signature if a Vet Center is listed in the boundary description.

Abstract

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

Area Columbia (CMO) is an Information Area that consists of Harry S Truman VAMC, Waynesville CBOC, Jefferson City CBOC, Kirksville CBOC, Mexico CBOC, Sedalia CBOC, St. James CBOC, Marshfield CBOC, Camdenton CBOC, Buttonwood CBOC, and Columbia Vet Center (CVC). The Area environment consists of components such as workstations, laptops, portable computing devices, terminals, servers, printers, and IT enabled networked medical devices that are owned, managed, and maintained by the facilities. The Area provides operational connectivity services necessary to enable users' access to information technology resources throughout the enterprise including those within the facility, between facilities, resources hosted at data centers, and connectivity to other systems. Network connectivity rules are enforced by VA approved baselines for router and switch configurations. The Area system environment also includes as applicable, subsystem storage utilities such as disk drives, network attached storage (NAS), storage area networks (SAN), archival appliances, special purpose systems, and tier 2 storage solutions. The Area encompasses the management, operational, and technical security controls associated with IT hardware, consisting of servers, routers, switches, hubs, gateways, peripheral devices, desktop/laptops, and OS software. The Area employs a myriad of routers and switches that connect to the VA network.

Overview

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

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

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

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

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

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

NOTE: If the SORN needs to be updated, please do not give the System of Records the same name as the IT system. SORNs should be technology-neutral – they pertain to the information within the IT system, not the IT system itself.

The applicable SORs for Area Columbia include:

Applicable SORs

Site Type: VHA 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 • Health Care Provider Credentialing and Privileging Records-VA¸SOR 77VA10E2E • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10 • Income Verification Records-VA, SOR 89VA10 • Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA13 • The Revenue Program Billings and Collection Records-VA, SOR 114VA10 • National Patient Databases-VA, SOR 121VA10 • Enrollment and Eligibility Records- VA 147VA10 • VHA Corporate Data Warehouse- VA 172VA10 • Health Information Exchange - VA 168VA005

Section 1. Characterization of the Information

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name
☒ Personal Mailing Address
Zip Code
☒ 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 (* See below)

*Area Columbia may collect additional PII/PHI as listed:

- Zip Code

PII Mapping of Components (Servers/Database)

Area Columbia consists of five (5) key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected within Area Columbia 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?

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

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

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

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

1.3 How is the information collected?

Means of Collection Table

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Legal Authority Table

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

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:

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

Mitigation:

VA Area Columbia employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control, awareness and training, audit and accountability, certification, accreditation, and security assessments, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and system and information integrity. The Area employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

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

Section 2. Uses of the Information

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

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

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

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

- **Vehicle License Plate Number**: Used for assignment of employee parking and assignment of parking during events
- **Internet Protocol (IP) Address Numbers**: Used for configuration and network connections. Network Communication allows information to be transferred from one Information Technology System to another.
- **Current Medications**: Used within the medical records for health care purposes/treatment, prescribing medications and allergy interactions.
- **Previous Medical Records**: Used for continuity of health care
- **Race/Ethnicity**: Used for patient demographic information and for indicators of ethnicity-related diseases.
- **Tax Identification Number**: Used for employment, eligibility verification
- **Medical Record Number**: Used to identify a patient within the medical record system without using their social security number as their identifier.
- **Next of Kin**: Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
- **Guardian Information**: Used when patient is unable to make decisions for themselves.
- **Electronic Protected Health Information (ePHI):** Used for history of health care treatment, during treatment and plan of treatment when necessary.
- **Military history/service connection**: Used to evaluate medical conditions that could be related to location of military time served. It is also used to determine VA benefit and health care eligibility.
- **Service-connected disabilities**: Used to determine VA health care eligibility and treatment plans/programs
- **Employment information**: Used to determine VA employment eligibility and for veteran contact, financial verification.
- **Veteran dependent information**: Used to determine benefit support and as an emergency contact person.
- **Disclosure requestor information**: Used to track and account for patient medical records released to requestors.
- **Death certificate information**: Used to determine date, location and cause of death.
- **Criminal background information**: Used to determine employment eligibility and during VA Police investigations.
- **Education Information**: Used for demographic background information for patients and as a determining factor for VA employment in areas of expertise. Basic educational background, e.g. High School Diploma, college degree credentials
- **Gender**: Used as patient demographic, identity and indicator for type of medical care/provider and medical tests required for individual.
- **Tumor PII/PHI Statistics**: Used to evaluate medical conditions and determine treatment plan

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

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

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

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

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

The VA Area Columbia uses statistics and analysis to create general reports that provide the VA a better understanding of *patient care, benefits, and employee needs*. These reports are:

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

These reports may track:

- The number of patients enrolled, provider capacity, staffing ratio, new primary care patient wait time, etc. for Veterans established with a Patient Care Aligned Team (PACT)
- Beneficiary travel summary/benefits

- Workload and cost resources for various services, i.e., mental health, primary care, home dialysis, fee services, etc.
- Daily bed management activity
- Coding averages for outpatient/inpatient encounters
- Satisfaction of Healthcare Experience of Patients (SHEP) data as it pertains to customer satisfaction regarding outpatient/inpatient services
- Unique patient trends
- Clinic wait times

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

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

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

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

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

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

Access to PII is determined by the position individuals hold within the facility. This is done by documentation and the assigning of a Functional Category to everyone in the facility using the VA Form 10-539 (Assignment of Functional Category). This form identifies the duty position of an individual and what access privileges they are authorized. The form is filled out by the supervisor/manager of the individual and the form is kept in the individual's personnel record at the facility and updated annually. Functional Category forms are audited by the Privacy Officer and Human Resources.

The controls in place to assure that the information is handled in accordance with the uses described above include mandatory online Information Security and Privacy and HIPAA training; face-to-face training for all incoming new employees conducted by the Information System Security Officer and Privacy Officer; regular audits of individuals accessing sensitive information; and formal

administrative rounds during which personal examine all areas within the facility to ensure information is being appropriately used and controlled.

Section 3. Retention of Information

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

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

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

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

The Area Columbia itself does not retain information.

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

- Current medications
- Gender
- Tax Identification Number
- Medical Record Number
- Vehicle License Plate Numbers

3.2 How long is information retained by the facilities?

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

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

Length of Retention Table

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

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

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

Retention Schedule Table

Site Type: VHA	***Retention Schedule***
VHA	Records Control Schedule 10-1 Records Control Schedule 005-1

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

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

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

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

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

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

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

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

Controls which are in place with regard to testing to minimize risk to privacy of using PII for testing include VA Technical Reference Model (TRM) Compliance Enforcement and Announcement of OIT Architecture and Engineering Review Board (AERB) VAIQ#7110943", dated July 1, 2011, compliance with the One-VA TRM is mandatory for any non-VA developed software which is deployed within VA's production network environment except for CIO exempted systems (i.e. medical devices), under VAIQ #7566605, Updated Security Requirements for Network Connected Medical Devices and Systems. This requirement is consistent with VA policy, including, but not limited to, VA Handbooks 6102 and 6500; VA Directives 6004, 6513, and 6517; and National Institute of Standards and Technology (NIST) standards, including Federal Information Processing Standards (FIPS). Regarding training all personnel on the facility staff or affiliated with the facility, who have access to PHI/PII are required to complete their privacy and information security training each year in an effort to minimize risk to privacy. For Research there are Data Use Agreements (DUA) in place with outside entities with whom the facility shares information with.
In the research department of the facility there is a deliberate review process for all human related study projects which includes review of the research projects by the Privacy Officer and the Information Systems Security Officer (ISSO) using VA checklists to ensure the research projects are compliant with VA requirements regarding PHI/PII.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

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

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

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

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

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

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT System***	***List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT System***	***Describe the method of transmittal***	***Applicable Sites within Area (VHA Program Office)***
Department of Veterans Affairs General Counsel	General Counsel	VA Patient Medical Records and all agency program office records to include Name, SSN, DOB, Mailing Address, Phone number, III, PHI, PII	Information may be transmitted upon request in an electronic, written, or verbal format based on the individual	Harry S Truman VAMC (VHA)
Veteran's Health Administration (VistA)	Electronic Health Record	Area boundary/System Log files to include Name, SSN, DOB, Mailing Address, Phone number, PHI, Area Boundary, System Log files, sample clinical.	Electronically pulled from VistA thru Computerized Patient Record System (CPRS)	Harry S Truman VAMC (VHA)
VHA Support Service Center (VSSC)	Capital Assets Management	Funding Information, Operational data, Basic statistics, Capital project tracking for the Veterans Health Administration (VHA), Clinical Specific Initiative (CSI) and Non-recurring Maintenance (NRM) Programs	Information may be transmitted upon request in an electronic, written, or verbal format based on the individual using VAEC (VA Enterprise Cloud) technologies	Harry S Truman VAMC (VHA)
Veterans Benefits Administration (VBMS)	Filing benefit claims	Personally Identifiable Information: Social Security Number, Benefits Information, Claims Decision, DD-214 (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).	Compensation and Pension Record Interchange (CAPRI) electronic software package	Harry S Truman VAMC- (VHA)
Austin Automation Center (AAC)	Offers common administrative	Certified security staff run our operations and	A program of enterprise "best	Harry S Truman VAMC- (VHA)

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT System*	*Describe the method of transmittal*	*Applicable Sites within Area (VHA Program Office)*
	services on a fee for service basis.	security is regularly reviewed by a variety of recognized commercial and Federal Information security specialists to include Name, SSN, DOB, Mailing Address, Phone number	practice" initiatives with major vendor partners that ensures customers receive enhanced, value-added IT services through the implementation of new technologies at competitive costs	
Veteran Service Organization (Veteran Center)	Veteran Center	Read only access to health information for plan of treatment to include Name, SSN, DOB, Mailing Address, Phone number.	Electronically pulled from VistA through Computerized Patient Record System (CPRS)	Harry S Truman VAMC- (VHA)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Privacy Risk: The internal sharing of data is necessary for individuals to receive benefits at Area Columbia. However, there is a risk that the data could be shared with an inappropriate VA

organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

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

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT System***	***List the specific data element types such as PII/PHI that are shared/received with the Program or IT System***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***	***Applicable Sites within Area (VHA Program Office)***
Abbott Laboratories	Medical Laboratory testing, diagnostics, maintenance, monitoring, and repair. Orders and results are communicated using a laboratory information system or middleware between instruments and VistA. VA owned sensitive information must not be physically moved or transmitted from the site without first obtaining prior written	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
	approval from the Information Owner and the data being encrypted prior to said move or transmission.				
Abbott Rapid Diagnostics Informatics Inc. (Formally Alere Informatics)	Data management. Diagnostics, maintenance, monitoring and repair. All communications described herein must be conducted in writing unless otherwise noted. No data is transmitted via VPN from VA to Abbott. Alere requires access to data management systems, located at numerous VAs via an	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)
	interconnection, as approved and directed by the Office of Information and Technology of VA. On a rare				

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
	occasion for troubleshooting purposes the data may include limited PHI datasets, e.g., patient name, test results, medical record number, full SSN, and accession number.				
Beckman Coulter, Inc.	Monitor system mechanical performance	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, FISMA	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)
Beckton-Dickinson, (Formerly CareFusion LLC Pyxis/Alaris)	Care of medical devices, all communications described herein must be conducted in writing unless otherwise noted. Monitoring information (CPU, memory, failure codes, etc.) remote control session traffic and files transfer. File transfer can contain PHI data,	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
	infusion event data, admissions discharge and transfer, usage/billing, and pharmacy medication order data. There is no PHI data sent from CareFusion to the VA.				
BioMerieux	Microbial Identification System. Can collect and store the following patient data: name, SSN, date of birth, gender, location, clinician, admission date. No PHI Data is stored externally by BioMerieux during normal support operations. All communications described herein must be conducted in writing unless otherwise noted.	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records, VA Handbook 6500	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)
Draeger Medical Inc.	Medical device monitoring and	Name, SSN, DOB, Address, phone	National ISA/MOU,	Site to Site (S2S), VPN	Harry S Truman

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
	troubleshooting etc. Transfer of raw data from machines through the concentrators that take the data and inputs into Phillips or ARK systems.	number, Race / Ethnicity, Gender	Privacy Act, HIPAA OMB, Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records		VAMC (VHA)
GE Healthcare (GEHC)	Maintenance and support of GE Healthcare Systems.	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender, Limited data sets with specific PHI elements depending on application	National ISA/MOU Privacy Act of 1974 HIPAA VA Handbook 6500	Site to Site (S2S), VPN includes tunneling, encryption, authentication and access control technologies and services	Harry S Truman VAMC (VHA)
Getwell Network **(Will soon change to Evideon**)	Patient Care Services, used for delivering education material to patients.	Name, Address	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records, VA Handbook 6500	Site to Site (S2S),	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
Merge Healthcare Solutions, Inc., formerly Ophthalmic Imaging Systems Inc (OISI)	Medical device monitoring and troubleshooting etc. All communications described herein must be conducted in writing unless otherwise noted. This information is not saved or copied by the Service Support unless there is a specific need to do so.	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)
Omnicell, Inc. (formally Aesynt)	Medication Dispensing and Supply. Collects and transfers data from the medication dispensing and supply cabinets via phone lines or a computer network.	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU Federal Information Security Management Act (FISMA) Health Insurance Portability and Accountability Act (HIPAA)	Site to Site (S2S), VPN connection. If VA transmits sensitive data to vendor over the system interconnection the transmission must be protected with FIPS 140-2 (or successor) validated encryption. The connections at each end are located within	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
				controlled access facilities using physical access devices and/or guards. Writing Mail or email, excluding any sensitive VA information. No VA sensitive information will be stored on Omnicell's systems.	
Office of Personnel Management Fingerprint Transaction System (OPM FTS)	The United States Office of Personnel Management (OPM) National Background Investigations Bureau (NBIB) conducts background investigations, reinvestigations, and continuous evaluations of individuals under consideration for, or retention of, Government employment. The purpose of the Fingerprint	Name, SSN, DOB, Facility Address, phone number, Race / Ethnicity, Gender, Name Social Security Number Date of Birth, Mother's Maiden Name Mailing Address, Zip Code Phone Number(s) Email Address Emergency Contact Information Certificate/License numbers	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records	T1, S2S, VPN Connection, Electronic Fingerprint capture/PIV ID Production for background checks	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
	Transaction System (FTS) is to provide a secure means for approved agencies to submit electronic or hard copy fingerprint images to the Federal Bureau of Investigation's Criminal Justice Information Services via NBIB's Federal Investigations Processing Center (FIPC). FTS contains Personally Identifiable Information (PII) about candidates who are undergoing a background investigation.	Previous Medical Records Current Medications, Military history /service connection, Service-connected disabilities. Employment information Vehicle License Plate Number Internet Protocol Address Numbers Tax Identification Number Disclosure Requestor Information Criminal Background Education Information			
Philips Healthcare (Formerly iSite/Stentor)	Support IntelliSpace CARE network. All communications described herein must be conducted in writing unless	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
	otherwise noted, Data transmitted from Philips to VA: Software updates, AV updates, configuration files Philips will have access to VA systems for the sole purpose of the operations as contractually agreed upon.		of certain medical records		
Quest Diagnostics, Inc.	Performing laboratory testing. HL7 Interface w/Data Innovations Server in Location. All communications described herein must be conducted in writing unless otherwise noted. Quest Diagnostics will have access to the PHI for the sole purpose of performing laboratory testing as contractually agreed upon. VA sensitive	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
	information will be stored on Quest Diagnostics' systems				
Roche Diagnostics	Chemistry Analysis. The Accu-Chek 360 Diabetes Management System allows for the collection, analysis and reporting of a diabetic user`s health information. The software functions with a compatible Accu-Chek blood glucose meter or insulin pump to monitor blood sugar, identify trends and compare medication, diet, and activity. This technology stores data in Microsoft Structured Query Language (SQL) Server. Data is	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records	Site to Site (S2S)	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
	transmitted to the storage repository by a local area network (LAN), Infrared (IR) reader, or Universal Serial Bus (USB) cable. A USB cable connects to a computer and an IR reader transfers data from meter to pump. Results can be exported into customized reports including support for the download and integration of blood sugar meter and insulin pump information onto a single graph.				
ScriptPro LLC / ScriptPro USA	Script scanning, Telepharmacy and Electronic Signature of patient for dispensed pharmacy products. If VA transmits sensitive data to	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
	vendor over the system interconnection, the transmission must be protected using FIPS 140-2 (or successor) validated encryption. The connections at each end are located within controlled access facilities using physical access devices and/or guards. Prescription data may include PII/PHI, Non-identifiable information, limited data set, de-identified information, Patient identifiers and unique Identifier from the ScriptPro SP Central system.		medical records		
Siemens Healthcare Diagnostics/	Imaging diagnostics for patients in need.	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU, Privacy Act,	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
Siemens Medical Solutions Inc.	Siemens requires access to data management systems, located at numerous VAs via an interconnection, as approved and directed by the Office of Information and Technology of VA. On a rare occasion for troubleshooting purposes the data may include limited PHI data sets, e.g., patient name, test results, medical record number, full SSN, and accession number.		HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records		
Sysmex America Inc.	Support Lab instruments. All communication must be conducted in writing, mail, or email, excluding any sensitive VA information unless otherwise noted. VA PHI	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
	will not be transmitted across the tunnel and any exposure by Sysmex's technical staff to VA PHI will be incidental.		medical records		
Topcon Medical Systems	Ophthalmology – Utilizes DICOM images to screen for remote support and maintenance. S2S VPN connection. If VA transmits sensitive data to vendor over the system interconnection, the transmission must be protected using FIPS 140-2 (or successor) validated encryption. The connections at each end are located within controlled	Name, date of birth and full SSN	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records	Site to Site (S2S)	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
	access facilities using physical access devices and/or guards.				
Vocera Communications, Inc (Formally Extension Healthcare)	The Vocera Communication System contains system intelligence, including user profiles, groups, call management, and call connections. The technology can interface with existing alarm and alert systems within a hospital to expedite communication of critical data.	User profiles, groups, location	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records	Site to Site (S2S), VPN, Internal communication throughout the hospital	Harry S Truman VAMC (VHA)
Welch-Allyn (a Hill-Rom Subsidiary)	Maintenance and Upgrades. This information is not saved or copied by the Service Support unless there is a specific need to do so.	Name, DOB, SSN and Address	National ISA/MOU, FISMA, HIPAA OMB, Privacy Act	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)
Wireless-Mobile1MD-PFTW	Internal Connections for the Pulmonary Function Test lab and associated	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	National ISA/MOU, Privacy Act, HIPAA Privacy Rule,	Vlan 445; BIOMED / Local OIT support	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
	testing equipment.		VA Claims Confidentiality Statute, Confidentiality of certain medical records		
Office of Personnel Management (OPM)	Manages civil service of the federal government, recruiting, health insurance, and retirement benefits programs. If VA transmits sensitive data to vendor over the system interconnection, the transmission must be protected using FIPS 140-2 (or successor) validated encryption. The connections at each end are located within controlled access facilities using physical access devices and/or guards	Name, address, SSN, medical data, service connection, gender, race, financial info., medical records, and employment records	National ISA/MOU, FISMA, HIPAA OMB Privacy Act, VA Claims Confidentiality Statute, Confidentiality of certain medical records	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
Social Security Administration (SSA)	Eligibility for Federal benefits	Name, SSN, DOB, Facility Address, phone number, Race / Ethnicity, Gender, Name Social Security Number Date of Birth, Mother's Maiden Name Mailing Address, Zip Code Phone Number(s) Email Address Emergency Contact Information Certificate/License numbers Previous Medical Records Current Medications, Military history /service connection, Service-connected disabilities. Employment information Vehicle License Plate Number Internet Protocol Address	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records, VHA Handbook 1605.01, Release of Information	Site to Site (S2S), IPSEC Tunnel, Secure FTP. Secure SSA website. S2S VPN connection. If VA transmits sensitive data to vendor over the system interconnection, the transmission must be protected using FIPS 140-2 (or successor) validated encryption. The connections at each end are located within controlled access facilities using physical access devices and/or guards.	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
		Numbers Tax Identification Number Disclosure Requestor Information Criminal Background Education Information			
University of Missouri, Department of Health Management and Informatics, Missouri Cancer Registry and Research Center (MCR-ARC)	Transmit and share sensitive data over the system interconnection to facilitate collaboration between Truman VAMC and MU. If VA transmits sensitive data to vendor over the system interconnection, the transmission must be protected using FIPS 140-2 (or successor) validated encryption. The connections at each end are located within controlled access	Name, full SSN, Date of Birth, medical information.	DUA (Data Use Agreement), MOU/ISA	Other- Business Partner Extranet, Air gapped, on-site VA premises	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
	facilities using physical access devices and/or guards.				
Department of Defense (DOD)	Determine military service dates, eligibility	Name, DOB, SSN, service connection, medical data	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records	Bi-directional Health Information Exchange	Harry S Truman VAMC (VHA)
Internal Revenue Service (IRS)	Income Verification	Name, SSN, financial Information	ISA/ MOU, Computer Matching Agreement	Secure Web-Portal, Secure Socket Layer	Harry S Truman VAMC (VHA)
Federal Emergency Management Agency (FEMA)	Emergency Operations, Disaster recovery	Name, Address, SSN, DOB, medical data, financial data	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records	Site to Site (S2S), VPN	Harry S Truman VAMC (VHA)

List External Program Office or IT System information is shared/received with	*List the purpose of information being shared / received / transmitted with the specified program office or IT System*	*List the specific data element types such as PII/PHI that are shared/received with the Program or IT System*	*List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*	*Applicable Sites within Area (VHA Program Office)*
Federal Bureau of Investigation (FBI)	Emergency Investigative Operations, Background Checks	Name, Address, SSN, DOB, medical data, financial data	National ISA/MOU, Privacy Act, HIPAA Privacy Rule, VA Claims Confidentiality Statute, Confidentiality of certain medical records	Site to Site (S2S)	Harry S Truman VAMC (VHA)
4D Medical MOU	The data will be transferred to and analyzed by 4DMedical with the intent to produce an anonymized DICOM wrapped X-ray Velocimetry Lung Ventilation Analysis Software (XV LVAS) report showing lung function and health	Name, SSN, DOB, Address, phone number, Race / Ethnicity, Gender	Local MOU	Site to Site (S2S), VPN, uses a system interconnection that is a direct connection between two or more information technology (IT) systems for sharing data and other information resources.	Harry S Truman VAMC (VHA)

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

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

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

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

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

Follow the format below:

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

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

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

Section 6. Notice

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

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

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

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

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

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

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

Applicable SORs

Site Type: VHA or Program Office	***Applicable SORs***
VHA	• Non-VA Fee Basis Records-VA, SOR 23VA10NB3 • Patient Medical Records-VA, SOR 24VA10A7 • Veteran, Patient, Employee, and Volunteer Research and Development Project Records- VA, SOR 34VA10 • Health Care Provider Credentialing and Privileging Records-VA¸SOR 77VA10E2E • Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SOR 79VA10 • Income Verification Records-VA, SOR 89VA10 • Automated Safety Incident Surveillance and Tracking System-VA, SOR 99VA131

Site Type: VHA or Program Office	*Applicable SORs*
	• The Revenue Program Billings and Collection Records-VA, SOR 114VA10 • National Patient Databases-VA, SOR 121VA10 • Enrollment and Eligibility Records- VA 147VA10 • VHA Corporate Data Warehouse- VA 172VA10 • Health Information Exchange - VA 168VA005

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

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

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

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

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

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

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

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

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

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

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

Notices (SOR) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

Section 7. Access, Redress, and Correction

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

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

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

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

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

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

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

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

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

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

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

The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA. Individuals are provided the opportunity to submit a request for change in their medical record via the amendment process. An amendment is the authorized alteration of health information by modification, correction, addition, or deletion. An individual can request an alteration to their health information by making a formal written request, mailed, or delivered, to the Privacy Officer at the VA health care facility that maintains the record. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. A decision to approve or deny the amendment request is made by the VA practitioner who entered the data, and this is relayed to the Veteran in writing by the facility Privacy Officer. Appeal rights are provided if a request is denied. The goal is to complete any amendment evaluation and determination within 30 days.

A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer (PO), or designee, to be date stamped; and filed appropriately. In reviewing requests to amend records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. That is, VA must maintain in its records only such information about an individual that is accurate, complete, timely, relevant, and necessary.

Individuals have the right to review and change their contact or demographic information at the time of appointment or upon arrival to the VA facility and/or submit a change of address request form to the facility business office for processing.

VA employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact the Contract Officer Representative to correct inaccurate or erroneous information upon request.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this Area and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be

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

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

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

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

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

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

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

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

Section 8. Technical Access and Security

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

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

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

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

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

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

Individuals receive access to the Area Columbia 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 Columbia requires access to the GSS be requested using the local access request system. VA staff must request access for anyone requiring new or modified access to the GSS. Staff are not allowed to request additional or new access for themselves.

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

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

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

Human Resources notify respective service lines, IT and ISSO of new hires and their start date(s), through email. The service line that the person is going into fills out the local access form, through an ePAS system 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 is routed through unique ePAS channels at the service line level, is signed by the service line Chief and Director, and then to IT for implementation.

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

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

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

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

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

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

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

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

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

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

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

8.4 Authorization and Accreditation (A&A) status

8.4a If Yes, provide:

1. *The Systems Security Plan Status**: Current***
2. *The Systems Security Plan Status Date**: September 24th 2024***
3. *The Authorization Status**: Current***
4. *The Authorization Date**: October 5, 2022***
5. *The Authorization Termination Date**: October 4, 2025***
6. *The Risk Review Completion Date**: October 3, 2024***
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): **Moderate***

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

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

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Privacy Officers

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

DOROTHEE SMITH Digitally signed by DOROTHEE SMITH
Date: 2025.02.06 12:32:46 -06'00'

Privacy Officer, Dorotheé C. Smith

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.

JULIE VANSTEENBURGH

Digitally signed by JULIE VANSTEENBURGH
Date: 2025.02.06 12:43:23 -06'00'

Information System Security Officer, Julie VanSteenburgh

Signature of Area Manager

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

JEFFREY SIMKINS Digitally signed by JEFFREY SIMKINS
Date: 2025.02.06 12:37:35 -06'00'

Area Manager, Jeffrey Simkins

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: VHA or Program Office	***Applicable NOPPs***
VHA	**https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946** **VHA Privacy and Release of Information:**

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 Mapping of Components (Servers/Database)

Components of the Area collecting/storing PII (*Each row refers to a grouping of databases associated with a single server****)***	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Applicable Sites within Area (VHA Program Office)***
Server 1 **Workstation for UPS** **• Shipping application**	Yes	Yes	Yes	Shipper/Recipient Name, Address, phone number	This data is needed to facilitate patient care	Advanced Encryption Standard (AES) 256, Server(s) is/are stored in a secured environment and managed with restricted access controls. (Bitlocker)	Harry S Truman VAMC (VHA)
Server 2 • Lynx Messenger • Lynx Key Pro	Yes	Yes	Yes	User location	Life-Safety (Code Orange)	Advanced Encryption Standard (AES) 256, Server is stored in a secured	Harry S Truman VAMC (VHA)

Components of the Area collecting/storing PII (*Each row refers to a grouping of databases associated with a single server****)***	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Applicable Sites within Area (VHA Program Office)***
						environment and managed with restricted access controls. (Bitlocker)	
Server 3 **• Police CCTV** **•Avigilon Control Center**	**Yes**	**Yes**	**Yes**	**CCTV Video Capture** **Surveillance, Audio, Patient information, facial recognition**	**Employee and patient safety**	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls. (Bitlocker)	**Harry S Truman** **VAMC (VHA)**
Server 4 **• Laurel Bridge Compass**	**Yes**	**Yes**	**Yes**	**Name, SSN, medical data**	**Medical imaging application for message routing, file transport, load**	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and	**Harry S Truman VAMC (VHA)**

Components of the Area collecting/storing PII (*Each row refers to a grouping of databases associated with a single server****)***	***Does this component collect PII? (Yes/No)***	***Does this component store PII? (Yes/No)***	***Does this component share, receive, and/or transmit PII? (Yes/No)***	***Type of PII (SSN, DOB, etc.)***	***Reason for Collection/ Storage of PII***	***Safeguards***	***Applicable Sites within Area (VHA Program Office)***
					balancing, and data extraction	managed with restricted access controls. (Bitlocker)	
Server 5 **• Rauland Nurse Call**	**Yes**	**Yes**	**Yes**	**Name, Last 4, Patient location, medical data**	**Nurse Call System**	Advanced Encryption Standard (AES) 256, Server is stored in a secured environment and managed with restricted access controls. (Bitlocker)	**Harry S Truman VAMC (VHA)**