Privacy Impact Assessment for the VA IT System called:

Enterprise VistA

Office of Information & Technology /Software Product Management (SPM)

Date PIA submitted for review:

January 12, 2022

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Kamilah Jackson</td>
<td><a href="mailto:kamilah.jackson@va.gov">kamilah.jackson@va.gov</a></td>
<td>(513) 288-6988</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Anita Feiertag</td>
<td><a href="mailto:Anita.Feiertag@va.gov">Anita.Feiertag@va.gov</a></td>
<td>(513) 475-6590</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Scott Madsen</td>
<td><a href="mailto:Scott.Madsen@va.gov">Scott.Madsen@va.gov</a></td>
<td>(801)-588-5237</td>
</tr>
</tbody>
</table>
Abstract

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

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

Overview

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

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes
- Whether the completion of this PIA could potentially result in technology changes.
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

Veterans Health Information Systems and Technology Architecture (VistA) is a comprehensive, full-featured Health Information System and Electronic Health Record (EHR) owned by the Veterans Health Administration (VHA) Office of Information Technology (OIT). VistA supports a large variety of clinical settings. Facilities range from small clinics that provide solely outpatient care to
large medical centers with significant inpatient populations and their associated specialties. The VistA modules focus on clinically relevant record keeping that improves patient care by improving clinical and administrative decision making. The Enterprise VistA Accreditation boundary consists of 128 VistA instances within 4 data centers. Enterprise VistA is utilized across VHA at more than 1,500 sites of care, supporting Veterans Affairs Medical Centers (VAMC), Community Based Outpatient Clinics (CBOC) and Community Living Centers (CLC), as well as at nearly 300 VA Vet Centers. Enterprise VistA serves America's Veterans by supporting exceptional quality health care. The VistA modules support a multitude of areas including medical and mental health treatment, medical imaging, supply management, decision support, medical research, and education. The purpose of the system is to collect, create, and maintain data about our VA employees, volunteers, business partners, and Veterans. The types of information include Protected Health Information (PHI) and Personally Identifiable Information (PII) data such as Demographics, Primary Contact, Medical/Mental Health, Criminal Background Information, Guardian, Benefits and Education. This system is authorized by 38 United States Code (USC) 7301(a)

The applicable SORNs are:
1. The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10A7 (Oct 2nd, 2020), in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf
2. The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA)-VA, SORN 79VA10 (Dec 12th, 2020), in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

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, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy-Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- Name
- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information
- Health Insurance Beneficiary Numbers Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Gender
- Integration Control Number (ICN)
- Military History/Service Connection
- Next of Kin
- Other Unique Identifying Information (list below)

Guardian
- Electronic Protected Health Information
- Medical/Mental health information
- Diagnosis(es)
- Procedure Codes
- Admission/treatment type
- Diagnostic results
- Service connection
- Service-connected disabilities
- Claim information to include payment and insurance
- Employment information
- Veteran dependent information
- Death certificate information
- Criminal background information
- Education information
- Medical statistics for research purposes containing PII/PHI

PII Mapping of Components
Enterprise VistA consists of 17 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Enterprise VistA and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**

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

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRAC Server</td>
<td>Yes</td>
<td>Yes</td>
<td>Patient Name, VA Master internal Entry Number (IEN), Person Index (MPI), Integration Control Number (ICN), SSN, Date of Birth (DOB), Sex, Diagnosis codes, Procedure codes, Admission Type, Date of care - Visit Date, Discharge Date, Most Recent Date of Care, Facility Name &amp; Station #, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Insurance, Billing data to include (charges, payments, claims processing, etc.) Medications, Provider Name, Biller Name</td>
<td>Electronic Health Record (EHR) and administrative functions to include employee and contractor data</td>
<td>Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information</td>
</tr>
<tr>
<td>Server Type</td>
<td>Access</td>
<td>Uses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>--------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ONTRAC Server</td>
<td>Yes</td>
<td>Patient Name, IEN, SSN, DOB, Sex, Diagnosis codes, Procedure codes, Admission Type, Date of care - Visit Date, Discharge Date, Most Recent Date of Care, Facility Name &amp; Station #, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Insurance, Billing data, Medications, Provider Name, Biller Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Electronic Health Record (EHR) and administrative functions to include employee and contractor data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Huron Test Server</td>
<td>Yes</td>
<td>Patient Name, IEN, SSN, DOB, Sex, Address/Phone #, Employer name/phone #, Diagnosis codes, Procedure codes, Admission Type, Date of care - Visit Date, Discharge Date, Most Recent Date of Care, Facility Name &amp; Station #, Rated Disabilities/Eligibility,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>YES</td>
<td>Electronic Health Record (EHR) and administrative functions to include employee and contractor data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------</td>
<td>-------------------------------</td>
<td>---------------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Veterans Services Server</td>
<td>Yes</td>
<td>Yes</td>
<td>Patient Name, IEN, SSN, DOB, Sex, Address/Phone #, Employer name/phone #, Diagnosis codes, Procedure codes, Admission Type, Date of care - Visit Date, Discharge Date, Most Recent Date of Care, Facility Name &amp; Station #, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Insurance, Billing data, Medications, Provider Name, Biller Name</td>
<td>Electronic Health Record (EHR) and administrative functions to include employee and contractor data</td>
<td>Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification, authentication, physical and environmental protection, system information</td>
</tr>
<tr>
<td>Enterprise Denials Server</td>
<td>Yes</td>
<td>Yes</td>
<td>Patient Name, IEN, SSN, DOB, Sex, Address/Phone #, Employer name/phone #, Diagnosis codes, Procedure codes, Admission Type, Date of care - Visit Date, Discharge Date, Most Recent Date of Care</td>
<td>Electronic Health Record (EHR) and administrative functions to include employee and contractor data</td>
<td>Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification, authentication, physical and environmental protection, system information</td>
</tr>
<tr>
<td>Payer Compliance Server &amp; Payer Compliance Test Server</td>
<td>Yes</td>
<td>Yes</td>
<td>Patient SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Type, Date of care - Visit Date, Discharge Date, Most Recent Date of Care, Facility Name &amp; Station #, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Insurance, Billing data to include (charges, payments, claims processing, etc.) Medications &amp; Provider</td>
<td>Electronic Health Record (EHR) and administrative functions to include employee and contractor data</td>
<td>Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information</td>
</tr>
<tr>
<td>Consolidated Mail Out Pharmacy (CMOP) Centralized Database (CDB)</td>
<td>Yes</td>
<td>Yes</td>
<td>Veteran's pharmaceutical prescription information is retained. Patient's name, address, SSN, RX number,</td>
<td>Electronic Health Record (EHR) and administrative functions to include employee</td>
<td>Access control, configuration management, media protection, system and service</td>
</tr>
<tr>
<td>Consolidated Mail Out Pharmacy (CMOP) Production Systems</td>
<td>Yes</td>
<td>Yes</td>
<td>Veteran's pharmaceutical prescription information is retained. Patient's name, address, SSN, RX number, type of medication, quantity ordered, instructions of use, physician's name, prescribing VAMC name, address and telephone number.</td>
<td>Electronic Health Record (EHR) and administrative functions to include employee and contractor data</td>
<td>Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information</td>
</tr>
<tr>
<td>Pharmacy (CMOP) Ensemble System</td>
<td>Prescription information is retained. Patient's name, address, SSN, RX number, type of medication, quantity ordered, instructions of use, physician's name, prescribing VAMC name, address and telephone number.</td>
<td>Record (EHR) and administrative functions to include employee and contractor data</td>
<td>Configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consolidated Mail Out Pharmacy (CMOP) Web Cancel Site</td>
<td>Yes</td>
<td>Yes</td>
<td>Veteran's pharmaceutical prescription information is retained. Patient's name, address, SSN, RX number, type of medication, quantity ordered, instructions of use, physician's name, prescribing VAMC name, address and telephone number.</td>
<td>Electronic Health Record (EHR) and administrative functions to include employee and contractor data</td>
<td>Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information</td>
</tr>
<tr>
<td>Location</td>
<td>Access Control</td>
<td>Functions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VistA Read-Only</td>
<td>Yes</td>
<td>Real-time copy of CPRS data to include: Name, SSN, DOB, Mother’s Maiden Name, Personal Mailing Address, Personal Phone Numbers, Personal Fax Number, Personal Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender, Next of Kin/Dependent information, Guardian, Electronic Protected Health Information, Military History, Service Connection, Service connected disabilities, Employment information and Death Certificate information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Austin Information Technology Center (AITC)</td>
<td>Yes</td>
<td>Electronic Health Record (EHR) and administrative functions to include employee and contractor data Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OI&amp;T</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>-----</td>
<td>-----</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Numbers, Personal Fax Number, Personal Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender, Next of Kin/Dependent information, Guardian, Electronic Protected Health Information, Military History, Service Connection, Service connected disabilities, Employment information and Death Certificate information

employee and contractor data

service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information

VistA cached copy, data to include: Name, SSN, DOB, Mother’s Maiden Name, Personal Mailing Address, Personal Phone Numbers, Personal Fax Number, Personal Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers/Account

Electronic Health Record (EHR) and administrative functions to include employee and contractor data

Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication
| Health Administration Center (HAC) | Yes | Yes | Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender, Next of Kin/Dependent information, Guardian, Electronic Protected Health Information, Military History, Service Connection, Service connected disabilities, Employment information and Death Certificate information | protection, awareness and training, identification authentication, physical and environmental protection, system information |
| DOB, Address, Sex, Diagnosis Codes, procedure Codes, Admission date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge, Insurance | Electronic Health Record (EHR) and administrative functions to include employee and contractor data | Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information |
| Health Eligibility Center (HEC) | Yes | Yes | Personally, identifiable information (PII) in the form of demographics such as: name, date of birth, social security numbers, race and gender; transient information such as phone numbers and addresses; Individually Identifiable Health Information (IIHI) to include diagnosis, treatment, payment, medication, and laboratory results | Electronic Health Record (EHR) and administrative functions to include employee and contractor data | Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information |
| Health Revenue Center (HRC) Topeka | Yes | Yes | DOB, Address, Sex, Diagnosis Codes, procedure Codes, Admission date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge, Insurance, Medication | Electronic Health Record (EHR) and administrative functions to include employee and contractor data | Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication |
| Veterans Benefits Administration (VBA) | Yes | Yes | Employee name & VistA menu options such as CPRS, ORLs, Claims and C&P exams | Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information |

1.2 What are the sources of the information in the system?

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

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
In general, we know that most, if not all VHA facilities will share data with internal VA programs and systems, including at a minimum:
• VA National Cemetery Administration (NCA)
• Veterans’ Benefit Administration (VBA)
• Consolidated Mail Out Pharmacy (CMOP)
• Consolidated Patient Accounts Center (CPAC)
• Veteran’s Benefit Administration (VBA)
• Health Eligibility Center (HEC)
• Health Revenue Center (HRC)
• Austin Information Technology Center (AITC)

Data, such as confirmation of military service or results of employee background checks, come from external Federal Agencies. These agencies include at a minimum:
• Department of Defense (DOD); Defense Health Agency (DHA)
• Internal Revenue Service (IRS)
• Office of Personnel Management (OPM)
• Social Security Administration (SSA)
• Federal Emergency Management Agency (FEMA)
• Federal Bureau of Investigation (FBI)

External sharing varies on a facility-by-facility basis and may for example share with the State Prescription Monitoring Program (SPMP), Research Partners, Departments of Health and private medical institutions.

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.
Information collected from individuals is collected verbally in interviews and conversations with VA medical and administrative staff, in writing (such as on VA Form 10-5345, Request for and Authorization To Release Medical Records Fillable), and via electronic and web form submissions.

Information is also collected from a variety of other IT systems and resources internal and external to the VA. These data collections may be completed using secure web portals and VPN connection.

Please review the Area PIAs for facility specific collection methods, including any information collected from state and local veterans’ organizations. https://www.oprm.va.gov/privacy/pia.aspx

1.4 How will the information be checked for accuracy? How often will it be checked?

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system 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 systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

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

Information obtained directly from the individual will be assumed to be accurate. Furthermore, individuals have the right to obtain access to their records and request correction to them when necessary (see Section 7 for additional information). Patient demographic as well as income verification matching completed by automated tools with connections to the Austin Information Technology Center (AITC) are obtained. Practitioners review and sign all treatment information and Business Office/Health Information Management Service reviews data obtained and assists with corrections.
Employee, contractor, students and volunteer information is obtained by automated tools as well as obtained directly by the individuals. The Federal Bureau of Investigation (FBI) and Office of Personnel Management (OPM) are contacted to obtain background reviews. Provider credentialing information is obtained from a variety of education resources.
Please review the individual PIAs for area specific information about information accuracy. https://www.privacy.va.gov/privacy_impact_assessment.asp

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?
List the full legal authority for operating the system, 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

Enterprise VistA, and all VHA facilities’ VistA instances operate under the authority of Veterans’ Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a). Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:


Additional information about state laws, local policies, and more can be found by reviewing the individual area Privacy Impact Assessments (PIAs). https://www.oprm.va.gov/privacy/pia.aspx System of Records Notice 79VA10A7– Veterans Health Information Systems and Technology Architecture & Patient Medical Records-VA, SORN 24VA10A7

1.6 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:** Enterprise VistA contains sensitive personal information – including social security numbers, names, and protected health information – on veterans, members of the public, & VA employees and contractors. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result.

**Mitigation:** Veterans Health Administration (VHA), Enterprise VistA, as well as the facilities deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors. Security measures include access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

**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 in the system 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.

The Enterprise VistA system boundary is comprised of facility level instances. Due to the extensive amount and nature of the information contained at each facility which can determine what information to collect, process, retain, or disseminate, a full understanding of the purpose for each individual data point can be obtained by reviewing the facility-level Privacy Impact. https://www.oprm.va.gov/privacy/pia.aspx

The records and information (e.g., Name, Social Security Number, Date of Birth, Mother’s Maiden Name, Mailing Address, Zip Code, Phone Number(s), Fax Number, Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers, Certificate/License Numbers, Internet Protocol (IP) Address Numbers, Current Medications, Previous Medical Records, Race/Ethnicity) may be used for statistical analysis to produce various management, workload tracking and follow-up reports; to track and evaluate the ordering and delivery of equipment, services and patient care; the planning, distribution and utilization of resources; the possession and use of equipment or supplies; the performance of vendors, equipment, and employees; and to provide clinical and administrative support to patient medical care.
The data may be used for research purposes. The data may be used also for such purposes as assisting in the scheduling of tours of duties and job assignments of employees; the scheduling of patient treatment services, including nursing care, clinic appointments, surgery, diagnostic and therapeutic procedures; the repair and maintenance of equipment and for follow-up activities to determine that the actions were accomplished and to evaluate the results; 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 systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

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

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

Patient and employee data are analyzed on an as-needed basis with tools relevant to the task at hand upon official authorization. Tools and applications used to analyze data will vary from facility to facility. Typically, statistics and analysis are utilized to create 3 types of general reports that provide the VA a better understanding of patient care and needs. The reports are:
1. Reports created to analyze statistical analysis on case mixes.
2. Analyze the number of places and geographical locations where patients are seen to assess the volume of clinical need.
3. Track and trend appointment availability and length data to track and trend average wait times.

Please reference the individual Privacy Impact Assessments for each facility to learn more.
https://www.oprm.va.gov/privacy/pia.aspx

To learn more about the above software visit https://www.va.gov/vdl/ for a complete list of the nationally released VistA Class 1 software packages.

2.3 How is the information in the system secured?
2.3a What measures are in place to protect data in transit and at rest? - Data in transit or at Rest is Encrypted

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? - In accordance with VHA Handbook 1605.02, access to SSNs is limited to employees for the necessity to conduct their job duties based on their assigned Functional Category. The SSN data at rest or SSN Data in use is encrypted. The function of the SSN is to identify the individual. The legal authority is Executive Order 9397, 38 USC section 501.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15? In accordance with VHA Handbook 1605.02, access to SSNs is limited to employees for the necessity to conduct their job duties based on their assigned Functional Category. The SSN data at rest or SSN Data in use is encrypted. The function of the SSN is to identify the individual. The legal authority is Executive Order 9397, 38 USC section 501.

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

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

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 system 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 system relevant to the mission of the project?

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

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

Prior to signing into VistA, system users are provided the below banner of Notice to User sign-on: VA systems are intended to be used by authorized VA network users for viewing and
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?

Identify and list all information collected from question 1.1 that is retained by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.
The records include information concerning current and former employees, applicants for employment, trainees, contractors, sub-contractors, contract personnel, students, providers and consultants, patients and members of their immediate family, volunteers, maintenance personnel, as well as individuals working collaboratively with VA. Below is a list of information that may be retained in the facility VistA instances:

• Name
• Social Security Number
• Date of Birth
• Mother’s Maiden Name
• Mailing Address
• Zip Code
• Phone Number(s)
• Fax Number Email Address
• Emergency Contact Information (Name, Phone Number, etc. of a different individual)
• Financial Account Information
• Health Insurance Beneficiary Numbers
• Account Numbers
• Certificate/License numbers
• Current Medications
• Previous Medical Records
• Race/Ethnicity

Please reference the facility-level Privacy Impact Assessment to learn more.
https://www.oprm.va.gov/privacy/pia.aspx

3.2 How long is information retained?

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 system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

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.


This document specifies how long records will be retained by the VA, if/when they will be transferred to a national records storage location, and the length of time the records will be stored at the national level. For greater details related to records retention, please review VA Handbook 6300.1 and RCS 10-1.

Below are some key record retention schedules for your information:
Health Record Folder File or Consolidated Health Record (CHR) contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a VA records storage facility.

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 (dated January 2019)).

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, Section 3020 Employee Management Records (GRS 2.2) (dated January 2019)).

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 Financial Management Section 4000 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf) for specific guidelines

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

When managing and maintaining VA data and records, healthcare facilities will follow the guidelines established in the NARA-approved Department of Veterans’ Affairs Record Control Schedule (RCS) 10-1 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf)

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

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

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans’ Affairs VA Directive 6371, Destruction of Temporary Paper Records (April 2014), https://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2. 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 VA Directive 6500, VA Cybersecurity Program, NIST SP 800-88 rev 1, Guidelines for Media Sanitization  https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf and the VA Media Sanitization User’s Guide (November 17, 2014). 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. Digital media is shredded or sent out for destruction based on the VA Media Sanitization User’s Guide. Additionally, Enterprise VistA and the facilities follow FSS Bulletin #209.1 National Media Sanitization and Destruction Program, as well as OIT-OIS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization

3.5 Does the system, where feasible, use 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

All IT system and application development and deployment is handled by VA OIT and authorized contracting staff. VHA does test new or modified IT systems for VHA operations prior to deployment, and PII/PHI may be used for that Alpha or Beta testing at the facility-level per VHA policy. In addition, VHA may need to train staff on functionality in the new or modified application(s). Training, including on IT systems, is part of health care operations and per VHA policy PII and PHI may be used for that training purpose. However, VHA must minimize the use of PII and PHI in training presentations or materials per VA policy. Where feasible, Veterans Affairs will use techniques to minimize the risk to privacy of using PII for research, testing and training.

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 system.

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

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

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

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

Follow the format below:

**Privacy Risk:** There is a risk that the information contained in the Enterprise VistA facility instances will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

**Mitigation:** In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary.

**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 is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

**NOTE:** Question 3.9 (second table) on 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 system 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 your program office, 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 with Internal Organizations

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veterans Health Administration (VHA)</td>
<td>Consolidated Patient Accounts Center (CPAC)</td>
<td>Patient Name, SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications, Provider Name, CPAC Biller Name</td>
<td>Secure File Transfer Protocol (SFTP)</td>
</tr>
<tr>
<td>Veterans Health Administration (VHA)</td>
<td>Consolidated Mail Out Pharmacy (CMOP)</td>
<td>Patient Name, SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance,</td>
<td>VistA Mailman messaging</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Veterans Health Administration (VHA)</td>
<td>All VistA instances via VistA Read-Only</td>
<td>Real-time copy of CPRS data to include: Name, SSN, DOB, Mother’s Maiden Name, Personal Mailing Address, Personal Phone Numbers, Personal Fax Number, Personal Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender, Next of Kin/Dependent information, Guardian, Electronic Protected Health Information, Military History, Service Connection, Service connected disabilities, Employment information and Death Certificate information</td>
<td>Transmission Control Protocol (TCP) Secure Sockets Layer (SSL)</td>
</tr>
</tbody>
</table>

Office of Information & Technology (OI&T) | Austin Information Technology Center (AITC) | VistA shadow copy, data to include: Name, SSN, DOB, Mother’s Maiden Name, Personal Mailing Address, Personal Phone Numbers, Personal Fax Number, Personal Email Address, Emergency Contact Information, | Transmission Control Protocol (TCP) Secure Sockets Layer (SSL) |
<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Information &amp; Technology (OI&amp;T)</td>
<td>Veterans Data Integration and Federation Enterprise Platform (VDIF-EP)</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system. List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system.</td>
<td>Describe the method of transmittal.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Financial Account Information, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender, Next of Kin/Dependent information, Guardian, Electronic Protected Health Information, Military History, Service Connection, Service connected disabilities, Employment information and Death Certificate information.</td>
<td>Encryption Control Protocol (ECP) connection.</td>
</tr>
<tr>
<td>Health Eligibility Center (HEC)</td>
<td>Master Person Index (MPI)</td>
<td>Personally, identifiable information (PII) in the form of demographics such as: name, date of birth, social security numbers, race and gender; transient information such as phone numbers and addresses; Individually Identifiable Health Information (IIHI) to include diagnosis, treatment, payment, medication, and laboratory results.</td>
<td>Health Level 7 (HL7)</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Veterans Benefits Administration (VBA)</td>
<td>Compensation and Pension Record Interchange (CAPRI)</td>
<td>Employee name &amp; VistA menu options such as CPRS, ORLs, Claims and C&amp;P exams</td>
<td>Remote Procedure Control (RPC) broker</td>
</tr>
<tr>
<td>Health Revenue Center (HRC) - Topeka</td>
<td>Claims server</td>
<td>Patient Name, SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications,</td>
<td>Secure Shell (SSH) / Remote Procedure Broker Calls (RPC) broker</td>
</tr>
<tr>
<td><strong>VHA</strong></td>
<td>Enterprise Testing Service VMWare Database</td>
<td>Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number</td>
<td>ASCII over SSH, TCP</td>
</tr>
<tr>
<td><strong>VHA</strong></td>
<td>Veteran Identity/Eligibility Reporting System</td>
<td>Personally Identifiable Information (PII) and Protected Health</td>
<td>Electronically pulled from VistA thru</td>
</tr>
<tr>
<td>*VHA</td>
<td>My HealtheVet</td>
<td>Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>*VHA</td>
<td>Veterans Integrated Registries Platform</td>
<td>Patient electronic health record, may include: • Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number • Email Address • Current Medications • Previous Medical Records • Race/Ethnicity • Theatre of War • Date of Death</td>
<td></td>
</tr>
<tr>
<td>*VHA</td>
<td>Insurance Capture Buffer Web</td>
<td>Name, Address, SSN, DOB, and insurance information</td>
<td></td>
</tr>
<tr>
<td>*VHA</td>
<td>Electronic Data Interchange</td>
<td>Personally, Identifiable Information (PII) to include but not limited to Patient Name, Date of Birth and Social Security Number</td>
<td></td>
</tr>
<tr>
<td>*VHA</td>
<td>VEText (Text Message Appointment Reminders)</td>
<td>Patient name, IEN, phone number and appointment date &amp; time</td>
<td></td>
</tr>
<tr>
<td>*VHA</td>
<td>Clinical Data Repository/Health Data Repository</td>
<td>Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number</td>
<td></td>
</tr>
<tr>
<td>System Name</td>
<td>Description</td>
<td>Contains Information</td>
<td>Data Transfer Method</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>----------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Veterans Data Integration and Federation Enterprise Platform</td>
<td>Users login identifier, User ID, Name of User, Patient's Identifier (EDIPI), Query Action - what widgets the user accesses within Veteran EHR, Start and End Timestamps, Date of Audit, IP Address of Machine Where User is Logged In</td>
<td>HTTPS</td>
<td></td>
</tr>
<tr>
<td>Central Fee System</td>
<td>Name, SSN, Date of Birth (DOB), Mailing Address, Zip Code, Financial Account Information, Medical Records, VA claims Information, Healthcare Provider Taxpayer ID (TIN), Health Insurance Beneficiary Numbers, Military Service Data</td>
<td>Encrypted electronic message via mailman service in VISTA</td>
<td></td>
</tr>
<tr>
<td>Bed Management Solution</td>
<td>Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Email Address, Emergency Contact Information, Ward Name, Bed Name, Race/Ethnicity, Patient VA MPI Integration Control Number (ICN)/Internal Entry Number (IEN), Attending Physician, Admitting Diagnosis</td>
<td>VIA VistA Integration Adapter (VIA) / Medical Domain Web Services (MDWS)</td>
<td></td>
</tr>
<tr>
<td>Veterans Point of Service Kiosk</td>
<td>Personally Identifiable Information (PII) to include but not limited to Patient Name, Date of Birth and Social Security Number</td>
<td>HL-7</td>
<td></td>
</tr>
<tr>
<td>Claims Processing &amp; Eligibility System</td>
<td>Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number</td>
<td>Via secure file transfer protocol within the VA Network, FIPS 2.0</td>
<td></td>
</tr>
<tr>
<td><strong>VHA</strong></td>
<td><strong>Health Data Repository</strong></td>
<td>Names, emails, Address, social security numbers, Lab results, Vital Signs, Allergies, Allergy Assessments, and Outpatient Pharmacy Medications</td>
<td>Electronically pulled from VistA thru VAMC thru E-VIE (Enterprise VistA Interface Engine) thru JMS (Java Message Service) Queues thru CDS (Clinical Data Services) Message Mediator</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>VHA</strong></td>
<td><strong>Joint Legacy Viewer (JLV)</strong></td>
<td>Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity VA MPI Integration Control Number (ICN)/Internal Entry Number (IEN)</td>
<td>Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS)</td>
</tr>
<tr>
<td><strong>VHA</strong></td>
<td><strong>eHealth Exchange</strong></td>
<td>PII to include but not limited to Patient Name, Date of Birth and Social Security Number</td>
<td>HTTPS</td>
</tr>
<tr>
<td><strong>VHA</strong></td>
<td><strong>Veterans Personal Finance System</strong></td>
<td>SSN, Full Name, Gender, Date of Birth, Date of Death, Address, Phone Number, Email Address, Admission Date, Discharge Date</td>
<td>VistALink</td>
</tr>
<tr>
<td><strong>VHA</strong></td>
<td><strong>Referral Authorization System</strong></td>
<td>Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number</td>
<td>HL7</td>
</tr>
<tr>
<td><strong>VHA</strong></td>
<td><strong>Capacity and Performance Engineering Services</strong></td>
<td>Personally, Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable information is obtained from VistA, to include but not limited to Patient Name, Date of Birth</td>
<td>Fileman SFTP over TCP/IP</td>
</tr>
<tr>
<td>*VHA</td>
<td>Behavioral Health Laboratories</td>
<td>PII/PHI to include but not limited to Patient Name, Date of Birth and Social Security Number</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>*VHA</td>
<td>National Provider Identification Crosswalk</td>
<td>Personally Identifiable Information (PII) and Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number</td>
<td>Inbound HL7 - Outbound Mailman</td>
</tr>
<tr>
<td>*VHA</td>
<td>VistA Audit Solution</td>
<td>Personally Identifiable Information (PII), Protected Health Information (PHI) to include but not limited to Patient Name, Date of Birth and Social Security Number</td>
<td>FIPS 140-2 Encrypted TCP</td>
</tr>
<tr>
<td>*VHA</td>
<td>Portal for Electronic Third-party Insurance Recovery</td>
<td>Name, SSN, DOB, Mailing Address, Zip Code, Phone Number(s), Health Insurance Information</td>
<td>HL7 message exchange using TCP/IP protocol</td>
</tr>
<tr>
<td>*VHA</td>
<td>National Medical Information System</td>
<td>Name, Zip Code, SSN, DOB, Age, Gender, Race/Ethnicity, Patient Treatment information, Current procedure/test, Previous Medical records, Diagnostic codes, Procedure codes, Hospital visits, Pre-diagnostic health data</td>
<td>Mailman to the AITC z13 mainframe NMIS application queues.</td>
</tr>
<tr>
<td>*VHA</td>
<td>VistA Imaging</td>
<td>System Log files, cache log files, images, text files, clinical data, etc., PII/PHI to include but not limited to Patient Name, Date of Birth and Social Security Number</td>
<td>RPC Calls or web services over HTTPS using TLS version 1.2 encryption.</td>
</tr>
<tr>
<td>*VHA</td>
<td>Community Viewer</td>
<td>Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Email Address, Emergency Contact Information, Current Medications, Previous Medical Records</td>
<td>Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS).</td>
</tr>
<tr>
<td>VHA</td>
<td>Medical Care Cost Recovery (MCCR) – National Database (NDB)</td>
<td>Name, Account receivables information, Debt Collection information, billing information</td>
<td>Mailman</td>
</tr>
<tr>
<td>VHA</td>
<td>3D Wound Care Management Solution</td>
<td>Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Email Address, Emergency Contact Information, Current Medications, Previous Medical Records, Race/Ethnicity, Patient ICN/IEN</td>
<td>Electronically transmitted to/from VistA thru Computerized Patient Record System (CPRS) via RPC Broker and VistA Imaging via RPC Broker + Background Processor via Samba share</td>
</tr>
<tr>
<td>VHA</td>
<td>Abbott Point of Care Portal</td>
<td>Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Email Address, Emergency Contact Information, Current Medications, Previous Medical Records, Race/Ethnicity, Patient ICN/Internal Entry Number (IEN)</td>
<td>HL7 over TCP/IP</td>
</tr>
<tr>
<td>VHA</td>
<td>Accu-Chek 360</td>
<td>Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Email Address, Emergency Contact Information, Current Medications, Previous Medical Records, Race/Ethnicity, Patient ICN/Internal Entry Number (IEN)</td>
<td>RPC Broker</td>
</tr>
<tr>
<td>VHA</td>
<td>Anesthesia Record Keeper</td>
<td>Name, Social Security Number</td>
<td>HL7 over TCP/IP</td>
</tr>
<tr>
<td>VHA</td>
<td>Caribou CLC Suite</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------</td>
<td>-------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>VHA</td>
<td>Cerner Healthe Intent</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>VHA</td>
<td>Data Access Services</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>VHA</td>
<td>Epic Cadence Enterprise Scheduling</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>VHA</td>
<td>Logicare</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>VHA</td>
<td>Patient Advocate Tracking System</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>VHA</td>
<td>Praedico</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>VHA</td>
<td>PraediGene</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>VHA</td>
<td>Veterans Service Network</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------</td>
<td>------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>VHA</td>
<td>Clinical Assessment, Reporting and Tracking</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>VHA</td>
<td>IAM - Single Sign-On Internal</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>VHA</td>
<td>IAM - Provisioning</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>VHA</td>
<td>VistA - Pharmacy</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>VHA</td>
<td>VDIF Disruptive Behavior Reporting System</td>
<td>Name</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------</td>
<td>------</td>
<td>------------------------</td>
</tr>
<tr>
<td>VHA</td>
<td>eScreening</td>
<td>Date of Birth</td>
<td>Mailing Address</td>
</tr>
<tr>
<td>VHA</td>
<td>Surgery Risk Assessment Database</td>
<td>Date of Birth</td>
<td>Mailing Address</td>
</tr>
<tr>
<td>VHA</td>
<td>Standards and COTS Integration Platform (formerly BHIE)</td>
<td>Query parameters for clinical information containing the patient ID (VA Integration Control Number (ICN)) and the type of clinical data being requested such as Veteran or Primary Subject’s Personal Contact Information (name, address, telephone, etc.), service information, medical information, and benefit information</td>
<td></td>
</tr>
<tr>
<td>VHA</td>
<td>Laboratory System Reengineering PathNet</td>
<td>PII as needed for specimen identification – SSN, Date of Birth, Sex, Race, Name, Blood Type, any specimen-specific information such as type of specimen</td>
<td>HL7 via TCP/IP</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>VHA</td>
<td>Healthcare Claims Processing System</td>
<td>Patient Name, SSN, DOB, Address, Sex, Diagnosis codes, Procedure codes, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications,</td>
<td>HL7 via TCP/IP</td>
</tr>
<tr>
<td>VHA</td>
<td>Path and Lab Med</td>
<td>PII as needed for specimen identification – SSN, Date of Birth, Sex, Race, Name, Blood Type, any specimen-specific information such as type of specimen</td>
<td>HL7 via TCP/IP</td>
</tr>
<tr>
<td>VHA</td>
<td>Mental Health Suite</td>
<td>Patient demographic data, to include Global Assessment of Functioning scores via the Mental Health Form</td>
<td>HL7 via TCP/IP</td>
</tr>
<tr>
<td>VHA</td>
<td>Community Viewer</td>
<td>Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medication Previous Medical Records Race/Ethnicity Patient ICN/IEN</td>
<td>TCP/ HTTPS</td>
</tr>
</tbody>
</table>

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

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

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance. The access request process utilizing Electronic Permission Access System (eMASS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

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

VistA menus and security keys are assigned by an approved access request based on specific job or duty requirements with least privileges. This access is reviewed for appropriateness on a biannual basis.

VistA applies the sensitive record flag to all employee and any veteran record where the veteran requests the record be sensitized. The ISSO reviews VistA audit messages for any potential access abnormalities or violations.

VA Facilities complete a multitude of auditing functions based on VA Handbook 6500 guidelines. VA Facilities complete an in-depth audit of VistA accounts to include separated users, elevated privileges, file access, separation of duties, sensitive records, inactive accounts as well as adhoc reports upon request.

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 IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

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

For each interface with a system 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

<table>
<thead>
<tr>
<th>List External Program Office or IT System</th>
<th>List the purpose of information being shared/received/transmitted with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cerner</td>
<td>Cerner Corporation</td>
<td>Data consists of PII, and PHI with information such as patient name, DOB, SSN, veteran service information, family relation, and medical information.</td>
<td>Health Level 7 (HL7), HL7 Optimized (HLO) via Site to Site (S2S) Virtual Private Network (VPN) tunnel</td>
<td>National MOU/ISA</td>
</tr>
<tr>
<td>Defense Medical Logistics Standard Support</td>
<td>Departme ent of Defense</td>
<td>Patient Care &amp; Treatment Data Logistics Data to support Patient Care</td>
<td>Joint Network Protection Suite (J-NPS) and Local Enclave Interconnectio n</td>
<td>MedCOI MOU/ISA</td>
</tr>
<tr>
<td>DoD - Joint Legacy Viewer</td>
<td>Departme nt of Defense</td>
<td>Patient Care &amp; Treatment Data to support Patient Care</td>
<td>Bi-directional Health Information Exchange</td>
<td>MedCOI MOU/ISA</td>
</tr>
<tr>
<td>Commercial Off the Shelf</td>
<td>Integrates with VistA</td>
<td>Name, SSN, DOB, Mother’s Maiden Name, Personal</td>
<td>Health Level 7 (HL7), Secure File Transfer</td>
<td>MedCOI MOU/ISA</td>
</tr>
<tr>
<td>Software (COTS) modules to provide a full service Electronic Health Record (EHR)</td>
<td>Mailing Address, Personal Phone Numbers, Personal Fax Number, Personal Email Address, Emergency Contact Information, Financial Account Information, Health Insurance National ISA/MOU Health Level 7 (HL7), Secure File Transfer Protocol (SFTP), Transmission Control Protocol/Internet Protocol (TCPIP)</td>
<td>Protocol (SFTP), Transmission Control Protocol/Internet Protocol (TCPIP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Version Date: October 1, 2021
Page 43 of 59
5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

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

Follow the format below:

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

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

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 as an appendix. (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 system 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, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. Major changes are mailed out every three years to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis. The Department of Veterans Affairs provides additional notice of this system by publishing two System of Record Notices (SORNs):

1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN24VA10A7 (Oct 2nd, 2020), in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

2) The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10 (Dec 12th, 2020), in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

This Privacy Impact Assessment (PIA) also serves as notice of the Enterprise VistA System. 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.”

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

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

The Veterans’ Health Administration (VHA) as well as the individual facilities request only information necessary to administer benefits to veterans and other potential beneficiaries. While
an individual may choose not to provide information to the VHA, this will prevent them from obtaining the benefits necessary to them.

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

6.3 Do individuals have the right to consent to particular 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

VHA permits individuals to agree to the collection and to the consent to the use of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. If the individual does not want their information collected or used, then they do not sign the consent form.
In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices (NOPP) and conversations with VHA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PH and PHI only as legally permitted including obtaining authorizations were required.
Where legally required VHA obtains signed, written authorizations from individuals prior to releasing, disclosing or sharing PII and PHI.
Individuals have a right to restrict the disclosure and use of their health information.
Individuals have a right to deny the use of their health information and/or IIHI and for the purpose of research.
Individuals can request further limitations on other disclosures. A veteran, guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information. The facility can approve or deny these requests. However, if the request to provide information is accepted the facility must conform to the restrictions

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

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

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

Follow the format below:

**Privacy Risk:** There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans’ Health Administration and the local facilities prior to providing the information to the VHA.

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

Section 7. Access, Redress, and Correction

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

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

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

If the system is 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 system is not a Privacy Act system, 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.
There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans’ Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility’s Release of Information (ROI) office.

VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access. VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

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

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.

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

The procedure for correcting inaccurate or erroneous information begins with a Veteran requesting the records in question from Release of Information (ROI). The Veteran then crosses out the information they feel is inaccurate or erroneous from the records and writing in what the Veteran believes to be accurate. The request for amendment and correction is sent to the facility Privacy Office for processing.

The documents are then forwarded to the practitioner who entered the data by the facility Privacy Officer. The practitioner either grants or denies the request. Once the practitioner has reviewed the requested amendment the document goes to the practitioner’s supervisor for review. The Veteran is notified of the decision via letter by the facility Privacy Officer. The goal is to complete any evaluation and determination within 30 days.

Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative (COR) 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 Notice of Privacy Practice (NOPP) which states:
Right to Request Amendment of Health Information
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:
• File an appeal
• File a “Statement of Disagreement”
• Ask that your initial request for amendment accompany all future disclosures of the disputed health information
Information can also be obtained by contacting the facility ROI office.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
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 ensure data accuracy.

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

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction
Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this system 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 a Veteran does not know how to obtain access to their records or how to request corrections to their records and that the health record could contain inaccurate information and subsequently affect the care the Veteran(s) receive.

**Mitigation:** As discussed in question 7.3, the Notice of Privacy Practice (NOPP), is provided to all enrolled Veterans which discusses the process for requesting an amendment to ones’ records. The VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their medical records and other records containing personal information.

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

In addition, 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 system, and are they documented?

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

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. 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 system. 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 System Design and Development.
Access to facility working and storage areas is restricted to VA employees who must complete both the HIPAA and Information Security training. Specified access is granted based on the employee’s functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information System Security Officer (ISSO), local Area Manager (AM), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.
Access is requested per VA policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor and OIT 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.
Access to VistA requires multi-layer authentication. The individual first must authenticate with PIV through Windows Active Directory. Additionally, they are assigned unique Access and Verify Codes. VistA access is time limited with session timeout after a designated period of inactivity and/or automatic account lock out unsuccessful attempts. Once inside the system, individuals are authorized to access information on a need to know basis. Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.
Access to computer rooms at the health care facilities and data processing centers is generally limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Information in VistA may be accessed by authorized VA employees. Access to file information is controlled at two levels. The systems recognize authorized employees by series of individually unique passwords/codes as a part of each data message, and the employees are limited to only that information in the file which is needed in the performance of their official duties. Information that is downloaded from VistA and maintained on laptops and other approved government equipment is afforded similar storage and access protections as the data that is maintained in the original files. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at the health care facility, or an OIG office location remote from the health care facility, is controlled in the same manner.
Information downloaded from VistA and maintained by the OIG headquarters and Field Offices on automated storage media is secured in storage areas for facilities to which only OIG staff have access.
Paper documents are similarly secured. Access to paper documents and information on automated storage media is limited to OIG employees who have a need for the information in the performance of their official duties.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?
If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system 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.

Contracts are reviewed based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee). Per specific contract guidelines, contractors/subcontractors are authorized to use VA information systems or access to VA information in accordance with VA Handbook 6500.6, Contract Security Privacy Checklist. The appropriate background investigation must be initiated, and fingerprinting conducted. All users of VA information systems or VA information must complete required training, VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176). The user must accept the Rules of Behavior (ROB) to indicate that they have read, understood, and agree to abide by the ROB before access is provided to the VA information system or the VA information. Authorized users must complete and comply with this training on an annual basis. Privacy and HIPAA training (VA 10203) must be completed for access to ePHI. Certification that this training has been completed by all contractors must be provided to the VHA employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy. Contractors with VistA access must have an approved electronic access request on file and access reviewed with the same requirements as VHA employees.

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

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All VA employees who have access to VA information must complete the onboarding and annual mandatory Department-wide privacy and information security training. In addition, all employees who interact with patient sensitive medical information must complete the VA mandated privacy HIPAA training. Finally, all new employees receive face-to-face training by the facility Privacy Officer and Information System Security Officer (ISSO) during new employee orientation. The Privacy and ISSO also perform subject specific trainings on an as needed basis.
8.4 Has Authorization and Accreditation (A&A) been completed for the system?

*If Yes, provide:*

1. The Security Plan Status,
2. The Security Plan Status Date,
3. The Authorization Status,
4. The Authorization Date,
5. The Authorization Termination Date,
6. The Risk Review Completion Date,
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

*Please note that all systems containing SPI are categorized at a minimum level of “moderate” under Federal Information Processing Standards Publication 199.*

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

1. The Security Plan Status, Complete
2. The Security Plan Status Date, August 5th, 2021
3. The Authorization Status, One (1) – Year ATO
4. The Authorization Date, ---- September 24, 2021
5. The Authorization Termination Date, ---- September 24, 2022
6. The Risk Review Completion Date ----------August 13th, 2021
7. The FIPS 199 classification of the system ----------HIGH

**Section 9 – Technology Usage**

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

*If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).*

*This question is related to privacy control UL-1, Information Sharing with Third Parties.*
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

N/A

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

N/A

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A

9.4 NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

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

N/A
9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as “Bots” or Artificial Intelligence (AI).

N/A
### Summary of Privacy Controls by Family

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

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

KAMILAH M. JACKSON 105810
Digitally signed by KAMILAH M. JACKSON 105810
Date: 2022.01.24 12:00:51 -05'00'

Privacy Officer, Kamilah Jackson

ANITA M. FEIERTAG 240557
Digitally signed by ANITA M. FEIERTAG 240557
Date: 2022.01.20 11:34:14 -05'00'

Information Systems Security Officer, Anita Feiertag

Scott L. Madsen 309788
Digitally signed by Scott L. Madsen 309788
Date: 2022.01.14 12:07:51 -07'00'

Information Systems Owner, Scott Madsen
APPENDIX A-6.1

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).

The VA System of Record Notice (VA SORN) Patient Medical Records


The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA)