Privacy Impact Assessment for the VA IT System called:

OEHRM Joint EHR System (eMASS #1175)
Office of Electronic Health Record Modernization (OEHRM)

Date PIA submitted for review:

7/20/20

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>Rita Grewal</td>
<td><a href="mailto:Rita.Grewal@va.gov">Rita.Grewal@va.gov</a></td>
<td>202-632-7861</td>
</tr>
<tr>
<td>Information System Security Officer</td>
<td>Perry Ungson</td>
<td><a href="mailto:Perry.Ungson@va.gov">Perry.Ungson@va.gov</a></td>
<td>650-444-6444</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>John Short</td>
<td><a href="mailto:John.Short@va.gov">John.Short@va.gov</a></td>
<td>202-714-3732</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.

In June 2017, the Secretary of Department of Veterans Affairs (VA) decided to replace the current electronic health record (EHR) system, the Veterans Information Systems and Technology Architecture (VistA), with commercial off-the-shelf (COTS) EHR products managed by the Cerner Corporation. The goal of this initiative is to modernize the VA’s healthcare technology infrastructure while allowing to gain full interoperability with the Department of Defense (DoD). The Cerner EHR solutions allow the VA to replace many components that exist in VistA.

Overview

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

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes
- Whether the completion of this PIA could potentially result in technology changes
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?
- Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.
- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?

What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?

The purpose of the OEHRM Joint EHR System (Federal Enclave) is to replace the current EHR legacy system, VistA, with a COTS EHR product (Cerner Millennium), managed and hosted by the Cerner Corporation in Kansas City, MO. The DoD authorized MHS GENESIS (aka Federal Enclave or DHMSM EHR (DoD eMASS ID#1017)) for deployment to their Military Treatment Facilities (MTFs). The goal of this initiative is to modernize the VA’s healthcare technology infrastructure while allowing to gain full interoperability with the DoD. The Cerner EHR solutions allow the VA to replace many components that exist in VistA. This is a mission-critical system collects, processes, and distributes EHR longitudinally across the Military Health System (MHS), VA, TRICARE, and Veterans Health Administration (VHA) network of service providers, Federal, and State agencies for approximately 9.6 million DoD beneficiaries and 9.11 million VA healthcare enrollees, worldwide. The OEHRM Joint EHR System will be implemented and maintained by the VA Office of Electronic Health Record Modernization (OEHRM).

VA Office of Information Technology (OIT) Office of Information Security (OIS) will leverage the enterprise approved Authority-to-Operate (ATO) reciprocity memorandum of understanding (MOU), “Authority to Operate (ATO) Reciprocity”, dated January 24, 2018 to establish dual authorization of the Federal Enclave. The OEHRM Joint EHR System (VA eMASS ID#1175), also known as the Joint EHR Millennium System is the VA authorization boundary of the Federal Enclave to be implemented and maintained by the VA Office of Electronic Health Record Modernization (OEHRM) to maximize scarce cybersecurity resources for due diligence, instead of redundant and unnecessary testing and/or reauthorization of a DoD ATO system. The security artifacts and test results of MHS GENESIS (DoD eMASS ID#1017) for Cerner Millennium (core EHR) shall be accepted by the VA to support a VA issued ATO for the OEHRM Joint EHR System (VA eMASS ID#1175) in a dual authorization capacity. A Terms of Reference (TOR) outlining the agreed upon security expectations and risk tolerance levels has been fully executed between the Program Executive Office, Defense Healthcare Management Systems (PEO DHMS) and VA OEHRM. The VA has migrated VistA medical records into the Federal EHR Enclave and will be deploying the Cerner solution to VA Medical Centers (VAMCs) for the next 10 years.

VA Sites (medical centers, clinics, data centers, etc.) will be connected to the OEHRM Joint EHR System (Federal Enclave) located at Cerner Corporation in Kansas City, MO. The Joint Security Architecture (JSA) will be deployed at the VA Sites, allowing VA information to traverse the Defense Health Agency (DHA) Medical Community of Interest (Med-COI) network into the Federal Enclave (OEHRM Joint EHR System). The authority to connect (ATC) process is managed by the DHA and will be followed to interconnect all MTF and VAMC infrastructure, medical devices, and systems. A Memorandum of Agreement (MOA) was signed to outline the design concepts, core capabilities, and operational characteristics of the Med-COI network and security architecture to be
adopted for use by both Departments. The MOA outlines requirements for each Department to direct changes within their organization to support the deployment, implementation, and sustainment of the resulting environment. Additionally, an interconnection security agreement (ISA) was established to address requirements that outlines technical details of each system’s architecture and the EHRM-related connections between the Departments. It documents specific terms of development, management, operation, maintenance, security and termination of interconnections. It defines standards implemented to safeguard the confidentiality, integrity and availability of the connected systems and the data stored, processed and transmitted. The ISA also identifies applicable internal documents, policies and procedures of each Department and reconciles any differences to also extend the use of reciprocity where applicable. This allows a level of consistency for maintaining PII in all sites operating under the same controls and standards across the enterprise.

The citation of the legal authority to operate the OEHRM Joint EHR System as an electronic health record information is 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 ). In June 2017, the Secretary of Department of VA decided to replace the current EHR system, the VistA, with COTS EHR products managed by the Cerner Corporation. The goal of this initiative is to modernize the VA’s healthcare technology infrastructure while allowing to gain full interoperability with the DoD. Information is shared internally with the Veterans Benefits Administration (VBA), Bed Management System, VA Health Eligibility Center (HEC), Consolidated Patient Account Center (CPAC) and other internal systems further listed in 4.1. Information is also being shared externally with the Social Security Administration (SSA), Internal Revenue Service (IRS), Federal Bureau of Investigation (FBI), Centers for Disease Control (CDC) and other external systems further listed in 5.1.

The completion of this PIA will not result in circumstances requiring changes to business processes. Business process (clinical workflows) at the VA Sites will be re-engineered to accommodate the modernized EHR system to maximize healthcare delivery.

The completion of this PIA will not result in changes to technology. Technology evolution will be determined by healthcare delivery and business operation needs.

The following VA System of Record Notices (SORNs), which will be amended, applies to the OEHRM EHR System (Federal Enclave):

- SORN 24VA10P2 - Patient Medical Records-VA;
- SORN 79VA10P2 – Veterans Health Information Systems and Technology Architecture (VistA) Records-VA;
- SORN 100VA10NS10 – Patient Advocate Tracking System (PATS)-VA;
- SORN 113VA112 – Telephone Service for Clinical Care Records-VA;
- SORN 114VA10D – The Revenue Program-Billing and Collections Records-VA
The correspondent DoD SORN is EDHA 07, Military Health Information System. The standalone MHS GENESIS SORN is being completed.

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.

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
- Other Unique Identifying Number (list below)

The following information are also included in the Joint EHR System database: Integration Control Number (ICN), EDIPI (Electronic Data Interchange Personal Identifier), education information, death certificate information, gender, Guardian information, Employment information, Veteran Dependent Information, and Disclosure Requestor information.

PII Mapping of Components
The OEHRM Joint EHR System (DHMSM EHR) consists of one (1) key component. The component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the OEHRM Joint EHR System (Federal Enclave) and the reasons for the collection of the PII are in the table below.

### PII Mapped to Components

<table>
<thead>
<tr>
<th>Components of the information system (servers) 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>OEHRM Joint EHR System (Federal Enclave)</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, SSN, EDIPI, Healthcare information (see details in answer 1.1)</td>
<td>Clinical care operation &amp; administration</td>
<td>Encryption, secure socket layer (SSL) virtual private network (VPN) tunnel</td>
</tr>
</tbody>
</table>

### 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.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Majority of the information is collected or created directly from the patients and inputted by individual users and clinical staff. For example: items such as names, social security numbers, date of birth are collected from the patient on healthcare enrollment forms, such as VA Form 10-10EZ as part of healthcare business operations.

Military service member information, such as dates of service, branch of service, type of discharge is collected by the DoD with cross-verification by Veterans Benefits Administration (VBA). In the case of a Veteran with a disability directly connected to their military service, the VBA may also provide service-connected disability ratings and information related to applicable disabilities (date granted, type of disability, overall percentage of combined disabilities). This data is populated directly from the VBA into OEHRM Joint EHR System (Federal Enclave) though secured methods. In cases where a Veteran has applied for a service-connected disability, but has not applied for VHA healthcare benefits, VBA will provide patient’s profile to facilitate the Compensation and Pension exam also through approved security measures.
mechanisms. This ‘patient profile’ will contain demographics such as the patient’s name, SSN, date of birth, and address. The information gathered about the patient using forms for the application for a service-connected disability but populated into the OEHRM Joint EHR System (MHS GENESIS) by an automated process connecting the VBA and VHA systems.

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 is collected directly from patients, providers, and various outside sources by the VA using several methods, such as paper forms (enrollment form for VA health care), interviews and assessments with the individual, secure web portals, virtual private network (VPN) connection, e-mail and facsimile, through various sources such as the DoD, VBA, Social Security Administration (SSA), and Internal Revenue Service (IRS). The DoD provides military records, including medical records compiled when the patient was a member of the United States (US) military. The VBA provides records which include the type and percentage of granted ‘service-connected’ disabilities, the dates of service-connected disability ratings, and, in some cases, the VBA populates patient demographics to provide a Compensation and Pension examination to a claimant. Income information is verified using information from the SSA and the IRS.

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

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

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose.

This question is related to privacy control AP-2, Purpose Specification.

Much of the information collected is maintained, used, and disseminated by the Federal Enclave (OEHRM Joint EHR System) to ensure that Veterans and other eligible individuals obtain the medical
and mental health treatment they require. Additional information, such as bank account information and insurance information are used to process claims and requests for benefits.

- Purposes of information collection, use, and dissemination include, but not limited to:
  - To determine eligibility for health care and continuity of care
  - Emergency contact information in cases of emergency situations such as medical emergencies.
  - Provide medical care
  - Communication with veterans/patients and their families/emergency contacts
  - Determine legal authority for providers and health care workers to practice medicine and/or subject matter expertise
  - Responding to release of information requests
  - Third party health care plan billing, e.g. private insurance
  - Statistical analysis of patient treatment

1.5 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 patient is assumed to be accurate. Information may be verified with other Federal agencies (DOD, SSA and IRS) to confirm eligibility or benefits. Should conflicting information exists, it will be documented and verified prior to further use.

Furthermore, individuals have the right to obtain access to their records and request correction to them when necessary (see Section 7 for additional information). Patient demographics as well as income verification matching are completed by automated tools. Practitioners review and sign all treatment information and Business Office/Health Information Management Service (HIMS) reviews data obtained and assists with corrections.

Employee, contractor, student and volunteer information is obtained by automated tools as well as directly from 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 educational resources.
1.6 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.

The legal authorities to operate this system are:

- **SORN 24VA10P2 - Patient Medical Records-VA;**
- **SORN 79VA10P2 – Veterans Health Information Systems and Technology Architecture (VistA) Records-VA;**
- **SORN 100VA10NS10 – Patient Advocate Tracking System (PATS)-VA;**
- **SORN 113VA112 – Telephone Service for Clinical Care Records-VA;**
- **SORN 114VA10D – The Revenue Program-Billing and Collections Records-VA**
- **Veterans Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b)**
- **Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, §7301(a)**
- **38 U.S.C. 8111, Sharing of Department Veterans Affairs and Department of Defense Health Care Resources.**

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

**Principle of Purpose Specification:** Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.
Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:

The OEHRM Joint EHR System (DHMSM EHR) collects PII and a variety of SPI, such as PHI for the purposes of business operations and healthcare delivery for our Veterans and Military Service Members. The information is collected or created directly from the patients and inputted by individual users and clinical staff using various methods. Information is also collected through various secure data sharing mechanism as specified in section 1.3. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

Mitigation:

VA and DoD employ a variety of security measures to ensure that the information is not inappropriately disclosed or released. These measures include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. All security controls have been implemented in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 and applicable VA Directives. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation; consistent with VHA Directive 1605.2, Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information.

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.

- **Name**: Used to identify the patient during appointments and in other forms of communication
- **Social Security Number**: Used as a patient identifier and as a resource for verifying income Information with the Social Security Administration
- **Date of Birth**: Used to identify age and confirm patient identity
- **Mother’s Maiden Name**: Used to confirm patient identity
- **Mailing Address**: Used for communication, billing purposes and calculate travel pay
- **Zip Code**: Used for communication, billing purposes, and to calculate travel pay
- **Phone Number(s)**: Used for communication, confirmation of appointments and conduct Telehealth appointments
- **Fax Number**: used to send forms of communication and records to business contacts, Insurance companies and health care providers
- **Email Address**: used for communication and MyHealtheVet secure communications
- **Emergency Contact Information (Name, Phone Number, etc. of a different individual)**: Used in cases of emergent situations such as medical emergencies.
- **Financial Account Information**: Used to calculate co-payments and VA health care benefit eligibility
- **Health Insurance Beneficiary Account Numbers**: Used to communicate and bill third part
  Health care plans
- **Certificate/License numbers**: Used to track and verify legal authority to practice medicine and Licensure for health care workers in an area of expertise.
- **Internet Protocol (IP) Address Numbers**: Used for configuration and network connections. Network Communication allows information to be transferred from one Information Technology System to another.
- **Current Medications**: Used within the medical records for health care purposes/treatment, prescribing medications and allergy interactions.
- **Previous Medical Records**: Used for continuity of health care
- **Race/Ethnicity**: Used for patient demographic information and for indicators of ethnicity-related diseases.
- **Next of Kin**: Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
- **Guardian Information**: Used when patient is unable to make decisions for themselves.
- **Electronic Protected Health Information (ePHI)**: Used for history of health care treatment, during treatment and plan of treatment when necessary.
- **Military history/service connection**: Used to evaluate medical conditions that could be related to location of military time served. It is also used to determine VA benefit and health care eligibility.
- **Service-connected disabilities**: Used to determine VA health care eligibility and treatment plans/programs
- **Employment information**: Used to determine VA employment eligibility and for veteran contact, financial verification.
• Veteran dependent information: Used to determine benefit support and as an emergency contact person.
• Disclosure requestor information: Used to track and account for patient medical records released to requestors.
• Death certificate information: Used to determine date, location and cause of death.
• Criminal background information: Used to determine employment eligibility and during VA Police investigations.
• Education Information: Used for demographic background information for patients and as a determining factor for VA employment in areas of expertise. Basic educational background, e.g. High School Diploma, college degree credentials.
• Gender: Used as patient demographic, identity and indicator for type of medical care/provider and medical tests required for individual.
• EDIPI and/or ICN: used as primary identifier and patient identity matching.

The OEHRM Joint EHR System (MHS GENESIS) information is used for various business operations and healthcare delivery of our Veterans and Military Service Members. The data may also be used for, but not limited to research, public health, and population health purposes. It can also be used assisting in the scheduling of tours of duties, and job assignments of employees; the scheduling of patient treatment services, including nursing care, clinic appointments, surgery, diagnostic and therapeutic procedures; the repair and maintenance of equipment and for follow-up activities to determine that the actions were accomplished and to evaluate the results; the registration of vehicles and the assignment and utilization of parking spaces; to plan, schedule, and maintain rosters of patients, employees and others attending or participating in sports, recreational or other events (e.g., National Wheelchair Games, concerts, picnics); for audits, reviews and investigations conducted by staff of the health care facility, the Network Directors Office, VA Central Office (VACO), 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

The OEHRM Joint EHR System (Federal Enclave) uses statistics and analysis to create many types of general reports that provide a better understanding of patient care and needs. These reports are used by the staff and management to identify, track and trend performance in a variety of areas including access, patient satisfaction, financial indicators and many others. Patient and employee data are analyzed on an as-needed basis with tools relevant to the task at hand upon official authorization. This data is never placed into the record of any patients, but is often saved as part of staff performance such as:

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

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII 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.

Minimum necessary access to PII is determined by the user’s manager/supervisor (accountable individual) and using service for the purposes of performing official assigned duties. Criteria, procedures, controls, and responsibilities regarding PII access are well documented as part of the system ATO.
process in accordance with NIST SP 800-53 Rev 4 and VA Handbook 6500 – Risk management framework for the VA information systems – Tier 3: VA information security program. It’s also captured in the Privacy managed Functional Categories process and verified filed in the employee’s personnel files annually. The VA OEHRM, in collaboration with DHMSM PMO and the Federal Electronic Health Record Modernization (FEHRM), is responsible for assuring safeguards of PHI/PII in the Federal Enclave (OEHRM Joint EHR System). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

VA and DoD employ a variety of security measures to ensure that the information is not inappropriately disclosed or released. These measures include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. All security controls have been implemented in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST SP 800-37 and applicable VA Directives. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation; consistent with VHA Directive 1605.2, Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information.

Additionally, prior to signing into EHRM systems, the user is provided a banner of Notice to User Sign-On that states:

“VA systems are intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized for official business and limited personal use under VA policy. Information from this system resides on and transmits through computer systems and networks funded by the VA. All access or use constitutes understanding and acceptance that there is no reasonable expectation of privacy in the use of Government networks or systems. All access or use this system constitutes user understanding and acceptance of these terms and constitutes unconditional consent to review and action including (but not limited to) monitoring recording copying auditing inspecting investigating restricting access blocking tracking disclosing to authorized personnel or any other authorized actions by all authorized VA and law enforcement personnel. Unauthorized user attempts or acts to (1) access upload download change or delete information on this system (2) modify this system (3) deny access to this system (4) accrue resources for unauthorized use or (5) otherwise misuse this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal civil or administrative penalties.”

********************************************************************************
** WARNING ** WARNING ** WARNING
This U.S. Government computer system is for official use only. The files on this system include Federal records that contain sensitive information. All activities on this system may be monitored to measure network performance and resource utilization; to detect unauthorized access to or misuse of the system or individual files and utilities on the system, including personal use; and to protect the operational integrity of the system. Further use of this system
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 OEHRM Joint EHR System (DHSM EHR) follows national VA policies regarding information retention. The records include information concerning current and former employees, applicants for employment, trainees, contractors, sub-contractors, contract personnel, students, providers and consultants, patients and members of their immediate family, volunteers, maintenance personnel, as well as individuals working collaboratively with VA.

- Name
- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Mailing Address
- Zip Code
- Phone Number(s)
- Fax Number
- Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information
- Health Insurance Beneficiary Numbers
- Account Numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Gender as provided by the patient
- Self-Identified Gender Identity provided by the patient
- Name and contact information for Guardian as provided by the patient
- Military and service history as provided by the patient and/or VBA
- Employment information as provided by the patient
- Veteran dependent information as provided by the patient
- Education information as provided by the patient
- Medical statistics for research purposes containing PII/PHI
• Name and contact information for Next of Kin Service-Connected rating and disabilities (based on information provided by Veteran and/or VBA)
• Date of death as supplied by Next of Kin or provider
• Criminal background and dependent information as reported by patient and/or national databases
• EDIPI and/or DoD ICN

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.

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.

When managing and maintaining data and records in the Federal Enclave, the most conservative length of retention will be utilized between the VA and DoD. The following are some key record retention schedules:

• **Medical Records Folder File or CHR (Consolidated Health Record):** 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, https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf).

• **Financial Records:** Different forms of financial records are retained 1-7 years based on specific retention schedules. Please refer to RCS-10-1 https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf for specific guidelines.

• **VA OIT Records:** These records are created, maintained and disposed of in accordance with VA RCS-10-1. Additionally, under OMB and the National Archives and Records Administration (NARA) guidelines, this facility will reference the Records Management Resources within the General Records Schedule. These specific resources can be found at http://www.archives.gov/records-mgmt/grs/.

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.

Version Date: February 27, 2020
Page 15 of 43
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.

The OEHRM Joint EHR System (Federal Enclave) operates using two (2) NARA approved retention schedules:

- Department of Veterans Affairs, Records Control Schedule 10-1 January 2019 [https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf](https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf)
- Department of Veterans Affairs, Office of Information & Technology Record Control Schedule 005-1 (August 3, 2009) [https://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf](https://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.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.

Information within the OEHRM Joint EHR System (DHMSM EHR) is destroyed by the disposition guidance of RCS 10-1. Once the information retention period is reached, Record Management and OIT will develop a plan for disposal or deletion. The plan will be routed for approval and implementations through VA and the National Archives, and will be derived from the following existing guidance:

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 8, 2014)

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

Hard copy documents that qualify as official records are handled in accordance with the record control schedules listed previously. Any temporary records or those authorized for disposal by
the appropriate control schedule are stored in secure containers until contracted personnel can collect them and shred the documents inside in accordance with VA Directive 6371 Destruction of Temporary Paper Records. The contractors provide a certificate of destruction to Facility Management Service. The paper waste is collected and sent off for pulping. Any contractors performing the on-site shredding services are certified through the National Association for Information Destruction (NAID).

Information stored electronically will be disposed of in accordance with VA Handbook 6500.1 Electronic Media Sanitization. Information is removed from media using VA approved methods prior to storage devices leaving VA control. When this is not possible the devices are rendered unreadable. Once information is removed from media or media is rendered unreadable the media is sent via registered courier to a destruction facility where the media is destroyed in such a manner that information can no longer be recovered from it. A chain of custody is maintained through the destruction process and a certificate of destruction is maintained by the VA and destruction facility.

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.

Certain types of testing maybe conducted for new or modified applications or information systems prior to deployment. The usage of PII/PHI in those tests, if any, must comply with the Federal Regulations listed below. In addition, as part of health care operations, VHA may need to train staff on functionality of new/modified IT systems. If PII/PHI is used in training materials, applicable VA/VHA directives must be followed. PII can be used in researches approved by the VA Institutional Review Board (IRB).

The following Federal Regulations are applicable to minimize the risk:

- 38 USC 5702 -researcher(s) must submit a written request to the Record Management officer in charge, stating purpose and duration of using the records for;
- 38 USC 5701 applicable to names and addresses;
- 38 USC 7332, applicable to Drug Abuse, alcohol Abuse, HIV Infection, and Sickle Cell Anemia Records; HIPAA Privacy Rule; Privacy Act of 1974; and
- 38 CFR 1.488 applicable to Drug Abuse, Alcohol Abuse, HIV Infection, and Sickle Cell Anemia Records.
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 maintained by the OEHRM Joint EHR System (MHS GENESIS) could be retained for longer than is necessary to fulfill the Department missions. 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 Department missions, the disposition of data housed is based on standards developed by the NARA. To mitigate the risk posed by information retention, the OEHRM Joint EHR System (Federal Enclave) adheres to the VA RCS schedules for each category or data maintained. When the retention period for the record is reached, the records are disposed as described in section 3.4.
Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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 data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>VHA - Sensis</td>
<td>Clinical care</td>
<td>PII/PHI – clinical care data</td>
<td>TLS</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 data element types such as PII/PHI that are shared/received with the Program or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>VistA Lab System Interfaces</td>
<td>Clinical care</td>
<td>PII/PHI – patient medical test data</td>
<td>TLS/OPENLink</td>
</tr>
<tr>
<td>Veterans Data Integration &amp; Federation Enterprise Platform (VDIF-EP),</td>
<td>Clinical care administration</td>
<td>PII/PHI – clinical care administration data</td>
<td>TLS</td>
</tr>
<tr>
<td>Joint Health Information Exchange (Joint-HIE)</td>
<td>Clinical care</td>
<td>PII/PHI – patient medical data</td>
<td>TLS</td>
</tr>
<tr>
<td>Joint Legacy Viewer (JLV)</td>
<td>Clinical care</td>
<td>PII/PHI – clinical care data</td>
<td>TLS</td>
</tr>
<tr>
<td>VA Master Patient Index</td>
<td>Clinical care</td>
<td>PII/PHI – patient care data</td>
<td>TLS</td>
</tr>
<tr>
<td>My Health VA</td>
<td>Clinical care, patient portal</td>
<td>PII/PHI – patient care data</td>
<td>TLS</td>
</tr>
<tr>
<td>Bed Management System</td>
<td>Clinical care</td>
<td>PII/PHI – patient care data</td>
<td>TLS/OPENLink</td>
</tr>
<tr>
<td>Financial Management System (FMS)</td>
<td>Clinical care administration, eligibility</td>
<td>PII/PHI, financial data</td>
<td>TLS</td>
</tr>
<tr>
<td>Pharmacy CoPay</td>
<td>Clinical care, eligibility</td>
<td>PII/PHI, patient medical data &amp; financial data</td>
<td>TLS/OPENLink</td>
</tr>
<tr>
<td>VistA Blood</td>
<td>Clinical care</td>
<td>PII/PHI – patient medical data</td>
<td>TLS/OPENLink</td>
</tr>
<tr>
<td>Austin Information Technology Center (AITC) - Health Data Repository (HDS)</td>
<td>Clinical care administration</td>
<td>PII/PHI – clinical care administration data</td>
<td>TLS</td>
</tr>
<tr>
<td>AITC- Data Access Service (DAS)</td>
<td>Clinical care administration</td>
<td>PII/PHI – clinical care data</td>
<td>TLS</td>
</tr>
<tr>
<td>AITC- Corporate Data Warehouse (CDW)</td>
<td>Clinical care administration</td>
<td>PII/PHI – clinical care legacy &amp; administration data</td>
<td>TLS</td>
</tr>
<tr>
<td>AITC - Establishment Computer Software</td>
<td>Clinical care administration</td>
<td>PII/PHI – clinical care administration data</td>
<td>TLS</td>
</tr>
<tr>
<td>VBA</td>
<td>Death/Burial Benefit</td>
<td>Death certificates, veteran eligibility</td>
<td>Hard copy mailing or via secure email</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 data element types such as PII/PHI that are shared/received with the Program or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>VA Tumor Register</td>
<td>Tracking &amp; trending of diseases</td>
<td>Diagnosis &amp; procedures, tumor status, treatment outcome, survivor tracking, type of treatments, demographics, hormone, radiation, chemotherapy, problem lists</td>
<td>TLS</td>
</tr>
<tr>
<td>VA Network Authorization Office – Non-VA care payments.</td>
<td>Health/medical payment authorization</td>
<td>Demographics, diagnoses, medical history, service connection, provider orders, VHA recommendation/approval for non-VA care.</td>
<td>Fee Basis Claim System (FBCS) authorization software program.</td>
</tr>
<tr>
<td>VA Health Eligibility Center</td>
<td>Determine Veteran eligibility</td>
<td>Service dates, SSN, demographics, service connection</td>
<td>Scanned documents uploaded into shared software programs</td>
</tr>
<tr>
<td>Consolidated Patient Account Centers (CPAC)</td>
<td>Medical care cost recovery</td>
<td>Diagnosis, service connection, dates of service, health insurance information, demographics.</td>
<td>Electronically pulled from the EHR system</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:**
There is a risk that information may be shared with unauthorized VA programs/systems or data could be shared with an inappropriate VA organizations and institutions which could have a potentially damaging impact on privacy.

**Mitigation:**

Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities.

**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: This question is #7 in the Privacy Threshold Analysis.

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
<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received 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>Department of Defense (DOD)</td>
<td>Clinical care, benefit eligibility verification</td>
<td>PII/PHI related to clinical care administration &amp; eligibility verification</td>
<td>VA SORNs 121VA10P2 and 168VA10P2; MOU for Data Sharing</td>
<td>Electronic site to site (S2S) (Transfer Layer Security TLS, VPN); Paper via US Postal Service</td>
</tr>
<tr>
<td>Office of Personnel Management (OPM)</td>
<td>Benefit eligibility verification</td>
<td>PII related to benefit eligibility verification</td>
<td>National ISA/MOU</td>
<td>Electronic: S2S, Paper: facsimile or hard copies via routine mail.</td>
</tr>
<tr>
<td>Social Security Administration (SSA)</td>
<td>Benefit eligibility verification</td>
<td>PII related to benefit eligibility verification</td>
<td>National ISA/MOU</td>
<td>Electronic: S2S, Paper: facsimile or hard copies via routine mail.</td>
</tr>
<tr>
<td>Federal Bureau of Investigation (FBI)</td>
<td>Background investigation</td>
<td>PII related to background investigation</td>
<td>National MOU SORN 02VA135 SORN 79VA19</td>
<td>Electronic: encrypted S2S</td>
</tr>
<tr>
<td>Internal Revenue Service (IRS)</td>
<td>Income verification</td>
<td>PII, financial information related to income verification</td>
<td>VA SORN 147VA16</td>
<td>Electronic: encrypted S2S</td>
</tr>
<tr>
<td>Centers for Disease Control (CDC)</td>
<td>Population health, research, prevention</td>
<td>PII/PHI related to population health research &amp; health statistics</td>
<td>VA SORN 121VA10P2 and MOU</td>
<td>Electronic: encrypted S2S</td>
</tr>
</tbody>
</table>
If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

- In compliance with OMB Memoranda M-06-15 and M-06-16, security and privacy controls will be implemented for OEHRM Joint EHR System (Federal Enclave) as being documented in the VA Enterprise Mission Assurance Support Service (eMASS) system.

- System and information are categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization process PII is identified accordingly.

- The VA has disseminated policies which direct and guide the activities and processes performed by its administrations (VHA, VBA, National Cemetery Administration (NCA)), offices, facilities, and programs. The policies are periodically reviewed to ensure completeness and applicability.

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

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

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

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

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

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

Follow the format below:

**Privacy Risk:**
The sharing of data is justifiable and necessary for the medical care of individuals eligible to receive care at VAMC’s, community-based outpatient clinics (CBOC’s), and MTFs. However, there are risks with data being shared or disclosed inappropriately to external organizations or institutions that do not have a need-to-know or legal authority to access.

**Mitigation:**
The potential harm is mitigated by access controls, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation. Criteria, procedures, controls, and responsibilities regarding access are well documented as part of the system ATO process in accordance with NIST SP 800-53 Rev 4 and VA Handbook 6500 – Risk management framework for the VA information systems – Tier 3: VA information security program.

Additionally, the use of secure passwords, access for need to know basis, PIV cards, PIN, encryption and access authorization are all measures that are utilized within the facilities. Standing letters for information exchange, business associate agreements and memorandums of understanding between agencies and VA are monitored closely by the VHA Privacy Office and HIMS to ensure protection of information. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

**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. The NOPP (Appendix A) is given out when the Veteran enrolls or when updates are made to the NOPP copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.

The Department of Veterans Affairs provides additional notice of this system by publishing the following SORNs:


This PIA also serves as notice of the OEHRM Joint EHR System (Federal Enclave) as required by the eGovernment Act of 2002, Public Law 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.

Yes, individuals do have an opportunity to decline to provide information at any time. There is no penalty or denial of service should an individual decline to provide information.

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.

Individuals have the right to consent to the use of their information. Individuals are directed to use the 10-5345 Release of Information (ROI) form describing what information is to be sent out and to whom it is being sent to. Patients have the right to opt-out of VA facility directories. 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.

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 VA prior to providing the information.

**Mitigation:**
This risk is mitigated by the common practice of providing the NOPP) when Veterans apply for benefits. Additionally, new NOPPs are provided to beneficiaries and periodic monitoring is performed to check that the signed acknowledgment form has been scanned into electronic records. Additional mitigation is provided by making the System of Record Notices (SORNs) and PIA available for review online, as discussed in question 6.1 and the Overview section of this PIA.

**Section 7. Access, Redress, and Correction**

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

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

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

When requesting access to one’s own records, patients are asked to complete VA Form 10-5345a: Individuals’ Request for a Copy of their Own Health Information, which can be obtained...
from the medical center or online at [http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf](http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf). Additionally, veterans and their dependents can gain access to their EHR by enrolling in the myHealthEvet program, VA’s online personal health record. More information about myHealthEvet is available at [https://www.myhealth.va.gov/index.html](https://www.myhealth.va.gov/index.html). The SORNs are also listed in the Overview section of this PIA, which address record access, redress, and correction. Links to all VA SORNs can be found at [https://www.oprm.va.gov/docs/CurrentSORNList_4_29_20.pdf](https://www.oprm.va.gov/docs/CurrentSORNList_4_29_20.pdf)

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

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

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

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

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

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

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.

The SORNs listed in section 6.1, each discuss and notify members of the public of the procedures related to record access, redress, and correction. Links to all VA SORNs can be found at: http://www.rms.oit.va.gov/sor_records.asp. Individuals may request correction of their information by contacting a Medical Support Assistant, the Patient Advocate and/or the ROI Office. Individuals are provided verbal notice of amendment process by the PO and/or HIMS Chief at time of request.

Veterans are informed of the amendment process by many resources to include the 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

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.

A formal redress process via the amendment process is available to all individuals. In addition to the formal procedures discussed in section 7.2 to request changes to one’s health record, a
veteran or other VAMC patient who is enrolled in myHealthevet can use the system to make direct edits to their health records.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this 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 individuals whose records contain incorrect information may not receive notification of appointments prescription medications, or test results. Furthermore, incorrect information in a health record could result in improper diagnosis and treatments. Additionally, there is a risk that a patient may not know how to obtain access to their records or how to request corrections to their records.

Mitigation:
The OEHRM Joint EHR System (Federal Enclave) mitigates the risk of incorrect information in an individual’s records by verifying information when possible using the resources discussed in section 1.5. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient’s medical appointments.

Additionally, staff are informed of the importance of maintaining compliance with VA ROI policies and procedures and about the importance of remaining alert to information correction requests.

As per section 7.3, the NOPP, which every patient would sign prior to receiving treatment, discusses the process for requesting an amendment to one’s records. Beneficiaries are reminded of this information when the NOPP is mailed to them by VA Privacy Office.
Requests for amendments, deletions, revision of information must be submitted in writing by Veteran or duly authorized representative for processing via the facility Privacy Officer and in accordance with VHA Directives, procedures.

**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 the 377 possible combinations of Cerner Millennium roles is determined by the user’s manager/supervisor (accountable individual) and the Using Service for the purposes of performing official assigned duties. The currently 377 Cerner Millennium roles are listed below.

Access to the VA OEHRM program is restricted to VA employees and contractors who must complete both the Privacy and HIPAA Focused and Information Security training. Specified access is granted based on the employee/contractor functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information Security Officer (ISO), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information. Users submit access requests based on need to know and job duties. Supervisor, ISSO 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 the OEHRM Joint EHR System (Federal Enclave) requires multi-factor authentication. The individual first must authenticate through Windows Active Directory. The Joint EHR system access is time limited with session timeout after a designated period of inactivity and/or automatic account lock out unsuccessful attempts. Once authenticated the system, individuals are authorized to access information on a need to know basis based on least privilege and minimum necessary standards approved by supervisors.
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 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.

Contractors sign applicable confidentiality agreements and access is verified through the Contracting Officer’s Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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.
Personnel that will be accessing VA information or information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Security Awareness training which all personnel must complete via the VA TMS system. After the user’s initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. 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. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually.

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

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. 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.

The DHMSM EHR (eMASS ID#1017) was initially authorized for operation in March 2018. Subsequently, a new and full (three-year) Re-authorization was granted in May 2020, by DoD Authorization Officer (AO). The system was classified as high, in accordance with FIPS 199. Cerner Millennium is a DoD authorized component of the MHS GENESIS (Federal Enclave) Authority-to-Operate (ATO). VA OIT OIS will leverage the enterprise approved ATO reciprocity MOU, “Authority to Operate (ATO) Reciprocity”, dated January 24, 2018 to maximize scarce cybersecurity resources for due diligence, instead of redundant and unnecessary testing and/or reauthorization of a DoD ATO system.
## Section 9. References

### 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>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.

RITA K GREWAL
114938
Digitally signed by RITA K GREWAL 114938
Date: 2020.08.03 06:48:13 -04'00'

Privacy Officer, Rita Grewal

Perry W. Ungson 131548
Digitally signed by Perry W. Ungson 131548
Date: 2020.07.31 09:01:54 -07'00'

Information Security Systems Officer, Perry Ungson

John A. Short 229575
Digitally signed by John A. Short 229575
Date: 2020.08.03 11:22:13 -04'00'

Information System Owner, John Short
APPENDIX A-6.1

As referenced in Section 6, the following is the NOPP provided to patients.

Department of Veterans Affairs  
Veterans Health Administration  
NOTICE OF PRIVACY PRACTICES  
Effective Date September 30, 2019

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED OR DISCLOSED AND HOW YOU CAN GET ACCESS TO YOUR INFORMATION.

PLEASE REVIEW IT CAREFULLY
The Department of Veterans Affairs (VA), Veterans Health Administration (VHA) is required by law to maintain the privacy of your protected health information and to provide you with notice of its legal duties and privacy practices. VHA may use or disclose your health information without your permission for treatment, payment and health care operations, and when otherwise required or permitted by law. This Notice outlines the ways in which VHA may use and disclose your health information without your permission as required or permitted by law. For VHA to use or disclose your information for any other purposes, we are required to get your permission in the form of a signed, written authorization. VHA is required to maintain the privacy of your health information as outlined in this Notice and its privacy policies. Please read through this Notice carefully to understand your privacy rights and VHA’s obligations.

YOUR PRIVACY RIGHTS

Right to Review and Obtain a Copy of Health Information. You have the right to review and obtain a copy of your health information in our records. You must submit a written request to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. The VHA Privacy Office at Central Office in Washington, D.C. does not maintain VHA health records, nor past military service health records. For a copy of your military service health records, please contact the National Personnel Records Center at (314) 801-0800. The Web site is https://www.archives.gov/veterans/military-service-records/medical-records.html.

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 or health records.

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

• File an appeal.
• File a “Statement of Disagreement” which will be included in your health record
• Ask that your initial request for amendment accompany all future disclosures of the disputed health information.

Right to Request Receipt of Communications in a Confidential Manner. You have the right to request that we provide your health information to you by alternative means or at an alternative location. We will accommodate reasonable requests, as determined by VA/VHA policy, from you to receive communications containing your health information:

• At a mailing address (e.g., confidential communications address) other than your permanent address.
• In person, under certain circumstances.
Right to Request Restriction. You may request that we not use or disclose all or part of your health information to carry out treatment, payment or health care operations, or that we not use or disclose all or part of your health information with individuals such as your relatives or friends involved in your care, including use or disclosure for a particular purpose or to a particular person.

Please be aware, that because VHA, and other health care organizations are “covered entities” under the law, VHA is not required to agree to such restriction, except in the case of a disclosure restricted under 45 CFR § 164.522(a)(1)(vi). This provision applies only if the disclosure of your health information is to a health plan for the purpose of payment or health care operations and your health information pertains solely to a health care service or visit which you paid out of pocket in full. However, VHA is not legally able to accept an out of pocket payment from a Veteran for the full cost of a health care service or visit. We are only able to accept payment from a Veteran for co-payments. Therefore, this provision does not apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of your health information to a health plan for the purpose of receiving payment for health care services VA provided to you.

To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. If we agree to your request, we will honor the restriction until you revoke it unless the information covered by the restriction is needed to provide you with emergency treatment or the restriction is terminated by VHA upon notification to you.

NOTE: We are not able to honor requests to remove all or part of your health information from the electronic database of health information that is shared between VHA and DoD, or to restrict access to your health information by DoD providers with whom you have a treatment relationship.

Right to Receive an Accounting of Disclosures. You have the right to know and request a copy of what disclosures of your health information have been made to you and to other individuals outside of VHA. To exercise this right, you must submit a written request to the facility Privacy Officer at the VHA health care facility that provides your care.

Right to a Printed Copy of the Privacy Notice. You have the right to obtain an additional paper copy of this Notice from your VHA health care facility. You can obtain this Notice from the facility Privacy Officer at your local VHA health care facility. You may also obtain a copy of this Notice at the following website: http://www.va.gov/vhapublications.

Notification of a Breach of your Health Information. If a breach of any of your protected health information occurs, we will notify you and provide instruction for further actions you may take, if any.

Complaints. If you are concerned that your privacy rights have been violated, you may file a complaint with:

- The Privacy Officer at your local VHA health care facility. Visit this Web site for VHA facilities and telephone numbers http://www.va.gov/directory/guide/home.asp?isflash=1
- VA via the internet through “Contact the VA” at http://www.va.gov or by dialing 1-800-983-0936 or by writing the VHA Privacy Office (10A7) at 810 Vermont Avenue NW, Washington, DC 20420.
- The U.S. Department of Health and Human Services, Office for Civil Rights at http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html
- Complaints do not have to be in writing, though it is recommended. An individual filing a complaint will not face retaliation by any VA/VHA organization or VA/VHA employee.

When We May Use or Disclose Your Health Information without Your Authorization

Treatment. We may use and disclose your health information without your authorization for treatment or to provide health care services. This includes using and disclosing your information for:
• Emergency and routine health care or services, including but not limited to labs and x-rays; clinic visits; inpatient admissions
• Contacting you to provide appointment reminders or information about treatment alternatives
• Seeking placement in community living centers or skilled nursing homes
• Providing or obtaining home-based services or hospice services
• Filling and submitting prescriptions for medications, supplies, and equipment
• Coordination of care, including care from non-VHA providers
• Communicating with non-VHA providers regarding your care through health information exchanges
• Coordination of care with DoD, including electronic information exchange

NOTE: If you are an active duty service member, Reservist or National Guard member, your health information is available to DoD providers with whom you have a treatment relationship. Your protected health information is on an electronic database that is shared between VHA and DoD. VHA does not have the ability to restrict DoD’s access to your information in this database, even if you ask us to do so.

Examples:
1) A Veteran sees a VHA doctor who prescribes medication based on the Veteran’s health information. The VHA pharmacy uses this information to fill the prescription.
2) A Veteran is taken to a community hospital emergency room. Upon request from the emergency room, VHA discloses health information to the non-VHA hospital staff that needs the information to treat this Veteran.
3) A National Guard member seeks mental health care from VHA. VHA discloses this information to DoD by entering the information into a database that may be accessed by DoD providers at some future date.
4) A Veteran is seen by his community health care provider, who wants to review the Veteran’s last blood work results from his VHA Primary Care visit for comparison. The community health care provider uses a local health information exchange to request and receive the results from VHA to better care for the Veteran.

Payment. We may use and disclose your health information without your authorization for payment purposes or to receive reimbursement for care provided. This includes using and disclosing your information for:
• Determining eligibility for health care services
• Paying for non-VHA care and services, including but not limited to, CHAMPVA, Choice and fee basis
• Coordinating benefits with other insurance payers
• Finding or verifying coverage under a health insurance plan or policy
• Pre-certifying insurance benefits
• Billing and collecting for health care services provided by VHA
• Reporting to consumer reporting agencies regarding delinquent debt owed to VHA.

Examples:
1) A Veteran is seeking care at a VHA health care facility. VA uses the Veteran’s health information to determine eligibility for health care services.
2) The VHA health care facility discloses a Veteran’s health information to a private health insurance company to seek and receive payment for the care and services provided to the Veteran.
3) A Veteran owes VA $5000 in copayments for Non-Service-Connected care over two years. The Veteran has not responded to reasonable administrative efforts to collect the debt. VA releases information concerning the debt, including the Veteran’s name and address, to a consumer reporting agency for the purpose of making the information available for third-party decisions regarding such things as the Veteran’s credit, insurance, housing, banking services, utilities.

Health Care Operations. We may use or disclose your health information without your authorization to support the activities related to health care. This includes using and disclosing your information for:
• Improving quality of care or services
• Conducting Veteran and beneficiary satisfaction surveys
• Reviewing competence or qualifications of health care professionals
• Providing information about treatment alternatives or other health-related benefits and services
• Conducting health care training programs
• Managing, budgeting and planning activities and reports
• Improving health care processes, reducing health care costs and assessing organizational performance
• Developing, maintaining and supporting computer systems
• Addressing patient complaints
• Legal services
• Conducting accreditation activities
• Certifying, licensing, or credentialing of health care professionals
• Conducting audits and compliance programs, including fraud, waste and abuse investigations
• Performing process reviews and root cause analyses

**Examples:**

1) Medical Service, within a VHA health care facility, uses the health information of diabetic Veterans as part of a quality of care review process to determine if the care was provided in accordance with the established clinical practices.

2) A VHA health care facility discloses a Veteran's health information to the Department of Justice (DOJ) attorneys assigned to VA for defense of VHA in litigation.

3) The VHA health care facility Utilization Review Committee reviews care data, patient demographics, and diagnosis to determine that the appropriate length of stay is provided per Utilization Review Standards.

**Eligibility and Enrollment for Federal Benefits.** We may use or disclose your health information without your authorization to other programs within VA or other Federal agencies, such as the Veterans Benefits Administration, Internal Revenue Service, or Social Security Administration, to determine your eligibility for Federal benefits.

**Abuse Reporting.** We may use or disclose your health information without your authorization to report suspected child abuse, including child pornography; elder abuse or neglect; or domestic violence to appropriate Federal, State, local, or tribal authorities. This reporting is for the health and safety of the suspected victim.

**Serious and Imminent Threat to Health and Safety.** We may use or disclose your health information without your authorization when necessary to prevent or lessen a serious and imminent threat to the health and safety of the public, yourself, or another person. Any disclosure would only be to someone able to help prevent or lessen the harm, such as a law enforcement agency or the person threatened. You will be notified in writing if any such disclosure has been made by a VHA health care facility.

**Public Health Activities.** We may disclose your health information without your authorization to public health and regulatory authorities, including the Food and Drug Administration (FDA) and Centers for Disease Control (CDC), for public health activities. This includes disclosing your information for:

- Controlling and preventing injury, or disability such as hepatitis, tuberculosis, and product defects or
- Reporting communicable diseases
- Reporting adverse events disease, such as hepatitis, tuberculosis, and product defects or
- Reporting vital events such as births and deaths
- Enabling product recalls,
- Tracking FDA-regulated products

**Judicial or Administrative Proceedings.** We may disclose your health information without your authorization for judicial or administrative proceedings, such as when we receive an order of a court, such as a subpoena signed by a judge, or administrative tribunal, requiring the disclosure.

**Law Enforcement.** We may disclose your health information without your authorization to law enforcement agencies for law enforcement purposes when applicable legal requirements are met. This includes disclosing your information for:
• Identifying or apprehending an individual who has admitted to participating in a violent crime
• Reporting a death where there is a suspicion that death has occurred as a result of a crime
• Reporting Fugitive Felons
• Routine reporting to law enforcement agencies, such as gunshot wounds
• Providing certain information to identify or locate a suspect, fugitive, material witness, or missing person
• Investigating a specific criminal act.

**Health Care Oversight.** We may disclose your health information without your authorization to a governmental health care oversight agency (e.g., Inspector General; House Veterans Affairs Committee) for activities authorized by law, such as audits, investigations, and inspections. Health care oversight agencies include government agencies that oversee the health care system, government benefit programs, other government regulatory programs, and agencies that enforce civil rights laws.

**Cadaveric Organ, Eye, or Tissue Donation.** When you are an organ donor and death is imminent, we may use or disclose your relevant health information without your authorization to an Organ Procurement Organization (OPO), or other entity designated by the OPO, for determining suitability of your organs or tissues for organ donation. If you have not specified your donation preferences and can no longer do so, your family may make the determination regarding organ donation on your behalf.

**Coroner or Funeral Services.** Upon your death, we may disclose your health information to a funeral director for burial purposes, as authorized by law. We may also disclose your health information to a coroner or medical examiner for identification purposes, determining cause of death, or performing other duties authorized by law.

**Services.** We may provide your health information without your authorization to individuals, companies and others who need to see your information to perform a function or service for or on behalf of VHA. An appropriately executed contractual document, if applicable, and business associate agreement must be in place to ensure the contractor will appropriately secure and protect your information.

**National Security Matters.** We may use and disclose your health information without your authorization to authorized Federal officials for conducting national security and intelligence activities. These activities may include protective services for the President and others.

**Workers’ Compensation.** We may use or disclose your health information without your authorization to comply with workers’ compensation laws and other similar programs.

**Correctional Facilities.** We may disclose your health information without your authorization to a correctional facility if you are an inmate and disclosure is necessary to provide you with health care; to protect the health and safety of you or others; or for the safety of the correctional facility.

**Required by Law.** We may use or disclose your health information without your authorization for other purposes to the extent required or mandated by Federal law (e.g., to comply with the Americans with Disabilities Act; to comply with the Freedom of Information Act (FOIA); to comply with a Health Insurance Portability and Accountability Act (HIPAA) privacy or security rule complaint investigation or review by the Department of Health and Human Services).

**Activities Related to Research.** Before we may use health information for research, all research projects must go through a special VHA approval process. This process requires an Institutional Review Board (IRB) to evaluate the project and its use of health information based on, among other things, the level of risk to you and to your privacy. For many research projects, including any in which you are physically examined or provided care as part of the research, you will be asked to sign a consent form to participate in the project and a separate authorization form for use and possibly disclosure of your information. However, there are times when we may use your health information without an authorization, such as, when:

• A researcher is preparing a plan for a research project. For example, a researcher needs to examine patient medical records to identify patients with specific medical needs. The researcher must agree to use this information only to prepare a plan for a research study; the researcher may not use it to contact you or actually conduct the study.
researcher also must agree not to remove that information from the VHA health care facility. These activities are considered preparatory to research.

- The IRB approves a waiver of authorization to use or disclose health information for the research because privacy and confidentiality risks are minimal and other regulatory criteria are satisfied.
- A Limited Data Set containing only indirectly identifiable health information (such as dates, unique characteristics, unique numbers or zip codes) is used or disclosed, with a data use agreement (DUA) in place.

Military Activities. We may use or disclose your health information without your authorization if you are a member of the Armed Forces, for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, when applicable legal requirements are met. Members of the Armed Forces include Active Duty Service members and in some cases Reservist and National Guard members.

Example:
Your Base Commander requests your health information to determine your fitness for duty or deployment.

Academic Affiliates. We may use or disclose your health information without your authorization to support our education and training program for students and residents to enhance the quality of care provided to you.

State Prescription Drug Monitoring Program (SPDMP). We may use or disclose your health information without your authorization to a SPDMP in an effort to promote the sharing of prescription information to ensure safe medical care.

General Information Disclosures. We may disclose general information about you without your authorization to your family and friends. These disclosures will be made only as necessary and on a need-to-know basis consistent with good medical and ethical practices, unless otherwise directed by you or your personal representative. General information is limited to:

- Verification of identity
- Your condition described in general terms (e.g., critical, stable, good, prognosis poor)
- Your location in a VHA health care facility (e.g., building, floor, or room number)

Verbal Disclosures to Others While You Are Present. When you are present, or otherwise available, we may disclose your health information to your next-of-kin, family or to other individuals that you identify. Your doctor may talk to your spouse about your condition while at your bedside or in the exam room. Before we make such a disclosure, we will ask you if you object or if it is acceptable for the person to remain in the room. We will not make the disclosure if you object.

Verbal Disclosures to Others When You Are Not Present. When you are not present, or are unavailable, VHA health care providers may discuss your health care or payment for your health care with your next-of-kin, family, or others with a significant relationship to you without your authorization. This will only be done if it is determined that it is in your best interests. We will limit the disclosure to information that is directly relevant to the other person’s involvement with your health care or payment for your health care.

Examples of this type of disclosure may include questions or discussions concerning your in-patient medical care, home-based care, medical supplies such as a wheelchair, and filled prescriptions.

IMPORTANT NOTE: A copy of your medical records can be provided to family, next-of-kin, or other individuals involved in your care only if we have your signed, written authorization or if the individual is your authorized personal representative.

Other Uses and Disclosures with Your Authorization. We may use or disclose your health information for any purpose you specify in a signed, written authorization you provide us. Your signed, written authorization is always required to disclose your psychotherapy notes, if they exist. If we were to use or disclose your health information for marketing purposes, we would require your signed written authorization. In all other cases, we will not use or make a disclosure of
your health information without your signed, written authorization, unless the use or disclosure falls under one of the exceptions described in this Notice. When we receive your signed, written authorization we will review the authorization to determine if it is valid, and then disclose your health information as requested by you in the authorization.

Revocation of Authorization. If you provide us a signed, written authorization to use or disclose your health information, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your health information unless the use or disclosure falls under one of the exceptions described in this Notice or as otherwise permitted by other laws. Please understand that we are unable to take back any uses or disclosures we have already made based on your signed, written authorization.

When We Offer You the Opportunity to Decline the Use or Disclosure of Your Health Information

Patient Directories. Unless you opt-out of the VHA medical center patient directory when being admitted to a VHA health care facility, we may list your general condition, religious affiliation and the location where you are receiving care. This information may be disclosed to people who ask for you by name. Your religious affiliation will only be disclosed to members of the clergy who ask for you by name.

**NOTE:** If you do object to being listed in the Patient Directory, no information will be given out about you unless there is other legal authority. This means your family and friends will not be able to find what room you are in while you are in the hospital. It also means you will not be able to receive flowers or mail, including Federal benefits checks, while you are an inpatient in the hospital or nursing home. All flowers and mail will be returned to the sender.

When We Will Not Use or Disclose Your Health Information

Sale of Health Information. We will not sell your health information. Receipt by VA of a fee expressly permitted by law, such as Privacy Act copying fees or FOIA copying fees is not a “sale of health information.”

Genetic Information. We will not use or disclose genetic information to determine your eligibility for or enrollment in VA health care benefits.

Changes to This Notice. We reserve the right to change this Notice. The revised privacy practices will pertain to all existing health information, as well as health information we receive in the future. Should there be any changes to this Notice we will make a copy of the revised Notice available to you within 60 days of any change. The Notice will contain the effective date on the first page.

Contact Information. You may contact the Privacy Officer at your local VHA health care facility if you have questions regarding the privacy of your health information or if you would like further explanation of this Notice. The VHA Privacy Office may be reached by mail at VHA Privacy Office, Office of Health Informatics (10A7), 810 Vermont Avenue NW, Washington, DC 20420 or by telephone at 1-877-461-5038 (toll free).