SPLASH PAGE LANGUAGE

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

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements
under the Federal Information Security Management Act (FISMA).

VA HANDBOOK 6508.1: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," July 2015, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=810&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

Claims Processing & Eligibility (CP&E)

Veterans Health Administration
Office of Community Care

Date PIA submitted for review:

04/26/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michael Hartmann	Michael.Hartmann@va.gov	303.780.4753
Information System Security Officer (ISSO)	Timothy Lindsay	timothy.lindsay@va.gov	478.272.1210 x2849
Information System Owner	Christopher Brown	christopher.brown1@va.gov	202.270.1432

Abstract

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

The Claims Processing and Eligibility (CP&E) system is the primary claims processing system for Veteran Family Services (VFS) claims.

Overview

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

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

The CP&E system that is currently located in Region 6 is primarily used to process claims of healthcare provided to veterans, dependents and/or their family members. CP&E is a single instance, enterprise client/server system written in Massachusetts General Hospital Utility Multi-Programing System (MUMPS) that uses the basic components of VistA (Kernel, FileMan, etc.).

Benefits Coordination with Center for Medicare and Medicaid Services is performed through monthly E01/E02 messaging. These flat files communicate with TRICARE or other VFS beneficiaries who have indications of Medicare/Medicaid beneficiary status. The business follows guidelines established and those are:

- **Conduct Claimant Validation** - is the resolution of issues resulting from performing completeness checks, validating information, and verifying content for VA benefits including business and industry development benefits.

- **Determine Benefits Eligibility** - determines whether or not an applicant is a valid claimant for VA benefits. Includes a managed process for assessing and determining beneficiary entitlement to VA and non-VA medical care and treatment services, based on the enrollee's eligibility status. Determining an enrollee's eligibility status requires verification of military service, as well as the type and status of discharge from active service. It also includes a determination of eligibility that is made in response to a request for burial in a VA National Cemetery and includes a review for a capital felony or schedule 3 sexual offense.
- **Determine Allowable Services** - is the process for ascertaining the appropriate level of benefit services for beneficiaries based on established eligibility requirements (e.g., presence of a service-related condition and meeting defined income thresholds). Beneficiaries are provided a certain level of access to health care based on defined policies and regulations (e.g., predetermined priority groups). This includes ascertaining the benefits for services provided by Veterans Benefits Administration (VBA) and National Cemetery Administration (NCA).
- **Perform Enrollment** - involves all aspects of the enrollment processes for medical and services provided by VBA and NCA including beneficiary identity and administrative data management, beneficiary information gathering, annual enrollment review, and the use and maintenance of the beneficiary enrollment system.
- **Perform Registration** - is the process of registering the Veteran for medical services. Registration entails processing registrations at assigned health care facilities, assigning Veterans to preferred health care facilities, and establishing health record and fiscal accounts at facilities. The registration process supports bi-directional registration between the Department of Defense and the Department of Veterans Affairs. Entering basic demographic data into a common interface will create a unique patient file in both agencies' electronic health record systems.
- **Monitor Access Status** - tracks and reports the access state of Veterans and Veteran populations. Access status includes the current state and history of eligibility, enrollment, allowable services, and registration.
- **Establish Payee Set-up and Maintenance** - includes establishing and maintaining Federal and non-Federal payee information.
- **Perform Obligation Management** - records commitments (if applicable); Record obligations; Includes de-commitments/modifications, liquidating commitments, de-obligations/modifications, and liquidating obligations.

There are currently over 300 million individual records on file. The CP&E system is currently located in Region 6. This includes the beneficiary information, vendor information and all supporting information/data required for claim processing. Data sharing is limited to Financial Management System and Center for Medicare and Medicaid Services. The system is used only at the Health Administration Center (HAC) Office of Information Technology (OIT) Denver and the information is protected by a firewall and access is only approved by the Information Security Office.

A citation of the legal authority to operate the IT system.

The SORN numbers are listed below and the link to those SORN is
https://www.oprm.va.gov/privacy/systems_of_records.aspx

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records - VA (1/25/2021)

54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA (11/8/2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) - VA (12/23/2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018
147VA10, Enrollment and Eligibility Records - VA (8/17/2021)

The completion of this PIA will not impact the business process. The completion of this PIA will not impact the technology process. No modifications currently being performed on the system should result in a need to amend or revise any SORN. The system is not cloud based. If the production PII data were to be intentionally or unintentionally released it could result in identity theft of veterans, veteran's dependents, veteran's family members. Additionally, the system contains medical data that could be made public. The intentional or unintentional data beach could significantly impact veterans, veteran's dependents, veteran's family members, and the reputation of the entire Department of Veteran Affairs.

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☒ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone

Number, etc. of a different individual)
☐ Financial Account Information
☒ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Current Medications
☒ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☒ Gender
☒ Integration Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Other Unique Identifying Information (list below)

- Member Identification Number
- Patient Control Number
- Medical Record Identification Number
- Medical Record Number
- Health Insurance Numbers
- CPY and International Code Designator (ICD) Coded Billing Information
- Billed Amounts
- Other Health Insurance Information
- Other Health Insurance Paid Amounts
- Provider Name
- Provider NPI
- Provider Phone Number
- Provider Billing Address
- Provider Physical Address
- Provider Remit to Address [DoVA1]
- Provider Email
- Provider Patient Control Number
- Provider Taxonomy Information
- Healthcare Provider Taxonomy Code
- Provider Secondary Identification (State License Number, UPIN, Provider Commercial Number, Location Number)
- Health Information
- Prescription Information
- Claim Service Date
- Procedure Codes
- Procedure Date
- Images

PII Mapping of Components

CP&E consists of 3 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CP&E and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public-facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Multi-Programing System (MUMPS)	Yes	Yes	PII and PHI	Claims Processing	Encryption and Access is controlled

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.

Information comes from other systems within the VA, external healthcare providers, veterans, and/or their dependents/family members in order for the VA to be able to process claims and provide reimbursement to healthcare providers providing healthcare to eligible veterans and/or their dependents outside the VA network.

During the course of processing claims additional information related to the claim is created in the form of a Patient Document Identifier (PDI) for traceability to all related claims. This information is then output to Health Share and the Financial Management System (FMS) repository.

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 may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Once the information is obtained a PDI is created for traceability.

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

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

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

Information received is verified by the system to ensure the veteran and/or their dependents are eligible and/or authorized to receive the care outside the VA network and that the claim is valid and appropriate. Verification is done by Social Security Number (SSN) eligibility check for the veteran and/or beneficiary.

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

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

This system supports electronic payment of health care claims and ensures VA is not in violation of the Health Insurance Portability and Accountability Act (HIPAA). The rules for data sharing are clearly laid out in the transactions sets and must be followed to the letter or claims will fail to process.

References:
23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)

43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records - VA (1/25/2021)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA (11/8/2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) - VA (12/23/2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018
147VA10, Enrollment and Eligibility Records - VA (8/17/2021)
38 U.S.Code. § 501 – Veterans' Benefits Rules and Regulations
38 U.S. Code § 1703 - Contracts for hospital care and medical services in non-Department facilities
38 U.S. Code § 1720G - Assistance and support services for caregivers
38 U.S. Code § 1781 - Medical care for survivors and dependents of certain veterans
38 U.S. Code § 1787 - Health care of family members of veterans stationed at Camp Lejeune, North Carolina
38 U.S. Code § 1802 - CHILDREN OF VIETNAM VETERANS BORN WITH SPINA BIFIDA Sec. 1802 - Spina bifida conditions covered
38 U.S. Code 1812 Children of Women Vietnam Veterans Born with Certain Birth Defects - Covered Birth Defects 1813
38 U.S. Code 1813 Children of Women Vietnam Veterans Born with Certain Birth Defects - Health Care
38 U.S. Code § 1821 - Benefits for children of certain Korea service veterans born with spina bifida
Public Law 103–446, section 107 Veterans Education and Benefits Expansion Act of 2001"- Sec. 107. Expansion of work-study opportunities.

38 U.S. Code § 1724 - Hospital care, medical services, and nursing home care abroad
38 U.S. Code § 1725 - Reimbursement for emergency treatment
38 U.S. Code § 1728 - Reimbursement of certain medical expenses
38 U.S. Code § 1703 - Contracts for hospital care and medical services in non-Department facilities
38 U.S. Code § 1720 - Transfers for nursing home care; adult day health care Public Law 111–163 section 101. CAREGIVERS AND VETERANS' OMNIBUS HEALTH SERVICES ACT OF 2010- Sec. 101. Assistance and support services for caregivers.
References for 23VA16 SORN Non-VA Care (Fee) Records-VA
5 U.S.C. § 301 - Departmental regulations
26 U.S. Code § 61 - Gross income defined (a) (12) Income from discharge of indebtedness
38 U.S.C. 31 Foreign Medical Program
38 U.S. Code § 109 - Benefits for discharged members of allied forces
38 U.S. Code § 111 - Payments or allowances for beneficiary travel
38 U.S. Code. § 501 - VETERANS' BENEFITS Rules and regulations
38 U.S. Code § 1151 - Benefits for persons disabled by treatment or vocational rehabilitation

38 U.S. Code § 1703 - Contracts for hospital care and medical services in non-Department facilities
38 U.S. Code § 1705 - Management of health care: patient enrollment system
38 U.S. Code § 1710 - Eligibility for hospital, nursing home, and domiciliary care
38 U.S. Code § 1712 - Dental care; drugs and medicines for certain disabled veterans; vaccines
38 U.S. Code § 1717 - Home health services; invalid lifts and other devices
38 U.S. Code § 1720 - Transfers for nursing home care; adult day health care
38 U.S.C. § 1721 - POWER TO MAKE RULES AND REGULATIONS
38 U.S. Code § 1724 - Hospital care, medical services, and nursing home care abroad
38 U.S. Code § 1725 - Reimbursement for emergency treatment
38 U.S.C. § 1727 - PERSONS ELIGIBLE UNDER PRIOR LAW
38 U.S. Code § 1728 - Reimbursement of certain medical expenses
38 U.S.C. 1741-1743. Per Diem Grant- State Home
38 U.S. Code § 1781 - Medical care for survivors and dependents of certain veterans
38 U.S. Code § 1786 - Care for newborn children of women veterans receiving maternity care
38 U.S. Code § 1787 - Health care of family members of veterans stationed at Camp Lejeune, North Carolina
38 U.S. Code § 3102 - Basic entitlement-A person shall be entitled to a rehabilitation program
38 U.S. Code § 5701 - Confidential nature of claims
38 U.S. Code § 5724 - Provision of credit protection and other services
54VA10NB3, ‘‘Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files—VA’’
38 U.S. Code. § 501 - VETERANS’ BENEFITS Rules and regulations
38 U.S. Code § 1703 - Contracts for hospital care and medical services in non-Department facilities
38 U.S. Code § 1720G - Assistance and support services for caregivers
38 U.S. Code § 1781 - Medical care for survivors and dependents of certain veterans
38 U.S. Code § 1787 - Health care of family members of veterans stationed at Camp Lejeune, North Carolina 38 U.S. Code § 1802-CHILDREN OF VIETNAM VETERANS BORN WITH SPINA BIFIDA-Spina bifida conditions covered 1803, Sec. 1803 - CHILDREN OF VIETNAM VETERANS BORN WITH SPINA BIFIDA -Health care 1812, 38 U.S. Code 1812 Children of Women Vietnam Veterans Born with Certain Birth Defects - Covered Birth Defects 1813, 38 U.S. Code 1813 Children of Women Vietnam Veterans Born with Certain Birth Defects-Health Care 38 U.S. Code § 1821 - Benefits for children of certain Korea service veterans born with spina bifida Public Law 103–446, section 107 Veterans Education and Benefits Expansion Act of 2001"- Sec. 107. Expansion of work-study opportunities.
38 U.S. Code § 1724 - Hospital care, medical services, and nursing home care abroad
38 U.S. Code § 1725 - Reimbursement for emergency treatment
38 U.S. Code § 1728 - Reimbursement of certain medical expenses
38 U.S. Code § 1703 - Contracts for hospital care and medical services in non-Department facilities
38 U.S. Code § 1720 - Transfers for nursing home care; adult day health care
Public Law 111–163 section 101. CAREGIVERS AND VETERANS’ OMNIBUS HEALTH SERVICES ACT OF 2010- Sec. 101. Assistance and support services for caregivers.
References for 23VA16 SORN Non-VA Care (Fee) Records-VA
5 U.S.C. § 301 - Departmental regulations

26 U.S. Code § 61 - Gross income defined (a) (12) Income from discharge of indebtedness
38 U.S.C. 31 Foreign Medical Program
38 U.S. Code § 109 - Benefits for discharged members of allied forces
38 U.S. Code § 111 - Payments or allowances for beneficiary travel
38 U.S. Code. § 501 - VETERANS' BENEFITS Rules and regulations
38 U.S. Code § 1151 - Benefits for persons disabled by treatment or vocational rehabilitation
38 U.S. Code § 1703 - Contracts for hospital care and medical services in non-Department facilities
38 U.S. Code § 1705 - Management of health care: patient enrollment system
38 U.S. Code § 1710 - Eligibility for hospital, nursing home, and domiciliary care
38 U.S. Code § 1712 - Dental care; drugs and medicines for certain disabled veterans; vaccines
38 U.S. Code § 1717 - Home health services; invalid lifts and other devices
38 U.S. Code § 1720 - Transfers for nursing home care; adult day health care
38 U.S.C. § 1721 - POWER TO MAKE RULES AND REGULATIONS
38 U.S. Code § 1724 - Hospital care, medical services, and nursing home care abroad
38 U.S. Code § 1725 - Reimbursement for emergency treatment
38 U.S.C. § 1727 - PERSONS ELIGIBLE UNDER PRIOR LAW
38 U.S. Code § 1728 - Reimbursement of certain medical expenses
38 U.S.C. 1741-1743. Per Diem Grant- State Home
38 U.S. Code § 1781 - Medical care for survivors and dependents of certain veterans
38 U.S. Code § 1786 - Care for newborn children of women veterans receiving maternity care
38 U.S. Code § 1787 - Health care of family members of veterans stationed at Camp Lejeune, North Carolina
38 U.S. Code § 3102 - Basic entitlement-A person shall be entitled to a rehabilitation program
38 U.S. Code § 5701 - Confidential nature of claims
38 U.S. Code § 5724 - Provision of credit protection and other services
38 U.S. Code § 5727 – Definitions
38 U.S. Code § 7105 - Filing of notice of disagreement and appeal
38 U.S. Code § 7332 - Confidentiality of certain medical records
38 U.S.C. 8131-8137. Construction Grant- State Home
44 USC - PUBLIC PRINTING AND DOCUMENTS
Veterans Access, Choice, and Accountability Act of 2014
38 CFR 2.6 - Secretary's delegations of authority to certain officials (38 U.S.C. 512).
TITLE 45 CFR—Public Welfare Subtitle A—DEPARTMENT OF HEALTH AND HUMAN SERVICES-PART
160—GENERAL ADMINISTRATIVE
REQUIREMENTS
45 CFR Part 164 - SECURITY AND PRIVACY
4 CFR 103 - STANDARDS FOR THE COMPROMISE OF CLAIMS

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

Without the information the VA would be unable to reimburse providers for the care they provided. The information is directly relevant and necessary to accomplish the specific purposes of the program. The program does to the extent possible and practical, collect information directly from the individual and if not possible, will review the records on file. There are policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current.

Privacy Risk: If the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for all Veterans and their dependents.

Mitigation: OIT develops, disseminates and periodically reviews and updates access control policies and procedures. OIT has formally developed an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among other VA entities. The policies and procedures are reviewed on an annual basis by responsible parties and updated as needed.

Section 2. Uses of the Information

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

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

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

The information is needed to provide reimbursement to healthcare providers providing healthcare to eligible veterans and/or their dependents outside the VA network.

Name: Used to identify the eligible beneficiary
Social Security Number: Used to identify the eligible beneficiary
Address: Used to identify the eligible beneficiary and to send correspondence

1. Provides identity and access management services to both internal VA employees and contractors and to external end users that do not have a VA approved credential.
2. Manages the identities of individuals that access VA logical resources.
3. Authenticates users across the enterprise.
4. Authorizes/grants users' permissions to protected VA information assets.
5. Enforces access to protected VA information assets.
6. Adheres to Federal guidelines, mandates, and timelines for information security.
7. Enables the management and oversight of auditable events and reporting for integrated services.

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 system is used to analyze the number of claims processed for given periods of time and the amount spent providing the care. All claims are archived in the system using Program Document Identifiers (PDIs) based on individual's PII. When new records are created the system will display all records associated with the claimant for the user to review and update according to established policies. The data is also used to identify fraud, waste, and abuse.

2.3 How is the information in the system secured?

2.3a What measures are in place to protect data in transit and at rest?

The use of encryption and cryptographic controls for protection of information is the VA standards and employs authentication methods that meet the requirements for standards and regulatory requirements for DAR and are FIPS 140-2. PIV access is required for access to the Application. Data is encrypted at rest, in transit and in use

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

No

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

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

The use of encryption and cryptographic controls for protection of information is the VA standards and employs authentication methods that meet the requirements for standards and regulatory requirements for DAR and are FIPS 140-2. PIV access is required for access to the Application. Data is encrypted at rest, in transit and in use

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

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

The only use of this data is to pay claims for Health Care by providers and beneficiaries and to comply with HIPAA legal requirements. It is not a reporting system and only takes electronic data in, repackages it and makes it available to the sites in the field for the approved claims processors to process. Access to the information is provided on a need-to-know basis, requires receiving an appropriate security clearance, and requires a request for elevated privileges to be submitted and approved before being granted access to the database.

The systems of records notices are clear about the uses of information and the system is relevant to the mission of the project:

- 23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
- 24VA10A7, Patient Medical Records - VA (10/2/2020)

- 43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records - VA (1/25/2021)
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
- 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA (11/8/2021)
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) - VA (12/23/2020)
- 88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018
- 147VA10, Enrollment and Eligibility Records - VA (8/17/2021)

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

Name
Social Security Number
Date of Birth
Mailing Address
Zip Code
Phone Number
Fax Number
Email address
Emergency Contact Information (Name, Phone Number, etc. of a different individual)
Financial Account Information
Health Insurance Beneficiary Numbers Account numbers
Current Medications
Previous Medical Records

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

Claims Processing and Eligibility data is retained per National Archives and Records Administration (NARA)GRS 3.2, item Information System Security Records, page II-2-5, to provide historical reports and to be available as needed for investigations or other legal reasons. GRS 3.2, item 031. Covers User Identification, Profiles, Authorizations, and Password Files and at time of publication requires a 6-year retention period from time of user account termination. System logs are retained for one year unless needed for audit or investigation. Records involved with ensuring use of standard Federal and agency forms to support effective record-keeping and ensuring that Federal standard forms are available and used as appropriate to support Federal record-keeping requirements.

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

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

Retention schedules have been approved by the National Archives and Records Administration. National (NARA). NARA GRS 3.2, Information System Security Records to provide historical reports and to be available as needed for investigations or other legal reasons. GRS 3.2, item 031. covers User Identification, Profiles, Authorizations, and Password Files and at time of publication requires a 6-year retention period from time of user account termination. System logs are retained for one year unless needed for audit or investigation.

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

No records are currently being destroyed or eliminated at the end of the retention period and will be archived; will follow the National Archives and Records Administration (NARA) retention schedule when required. The retention schedules have been approved by the NARA. National Archives and Records Administration GRS 3.2, Information System Security Records to provide historical reports and to be available as needed for investigations or other legal reasons. GRS 3.2, item 031. covers User Identification, Profiles, Authorizations, and Password Files and at time of publication requires a 6-year retention period from time of user account termination. System logs are retained for one year unless needed for audit or investigation.

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

PII is not used during testing, training and research. There are policies and procedures in place addressing this matter and each member has training to ensure they understand the risks if used. Training documentation is kept within the Training office.

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.

Privacy Risk: The risk to maintaining data within the Identity Access Management system is that longer retention times increase the risk that information can be compromised or breached.

Mitigation: When the retention for the data collected is reached for a record, the IAM team will carefully dispose of the data; however, currently records are not being destroyed at this time due to the retention timeline defined in NARA. All electronic storage media used to store, process, or access VA Sensitive Information including PII will be disposed of in adherence with the latest version of VA Handbook 6500.1, Electronic Media Sanitization. In addition, OIT develops, disseminates and periodically reviews and updates access control policies and procedures. OIT

has formally developed an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among other VA entities. The policies and procedures are reviewed on an annual basis by responsible parties and updated as needed.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Community Care - Customer Relationship Management	Used to transmit data to and from the VBA and between the different systems.	Information about the patient, their eligibility to receive care, if they are authorized the care, and/or claim/billing information.	Via secure file transfer protocol within the VA network, paper, and/or by phone.

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Financial Management System	Used to transmit data to Treasury.	Claim billing and payment purposes by the VA.	Via secure file transfer protocol within the VA network, paper, and/or by phone.
Interactive Voice Response	Self-service option to check their most recent payment information.	Information about claims, benefits, education, Insurance, Pension, or other benefits offered.	Via secure file transfer protocol within the VA network, paper, and/or by phone.
VA Master Person Index (VA MPI)	The primary vehicle for assigning and maintaining unique patient identifiers.	The authoritative identity service within VA, establishing, maintaining, and synchronizing identities for Veterans.	Via secure file transfer protocol within the VA network, paper, and/or by phone.
Program Integrity Tool	Used for processing veteran claims.	A repository with a claims scoring tool that will score incoming claims for risk of fraud, waste and abuse.	Via secure file transfer protocol within the VA network, paper, and/or by phone.
Veterans Affairs/Department of Defense Identity Repository (VADIR)	Information Sharing	ALL ALL-Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Provider's TIN and Address information.	Via secure file transfer protocol within the VA network
Veteran Identity/Eligibility Reporting System	System enables applications to search records and retrieve profile data, military history, and information on compensation and benefits, disabilities, and dependents.	Provide consuming business applications with access to a standard, enterprise view of person demographic, contact, military service and other benefits information.	Via secure file transfer protocol within the VA network, paper, and/or by phone.

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Veterans' Health Information System and Technology Architecture	This is the system of record for most of the claims data.	Information about the patient, their eligibility to receive care if they are authorized the care, and/or claim/billing information.	Via secure file transfer protocol within the VA network, paper, and/or by phone.
ODM	A business rules engine that supports automated decision-making for FMP claims.	Information about the patient, their eligibility to receive care if they are authorized the care, and/or claim/billing information.	Via SOAP and secure file transfer protocol within the VA network
My HealtheVet	Web enabled health information portal for veterans.	Information about claims, benefits, education, Insurance, Pension, or other benefits offered.	Via secure file transfer protocol within the VA network
McKesson Claim Check	Claim auditing software	Eligibility data	Via SOAP and Enterprise Cache Protocol within the VA network.
PED Cloud	Used for processing veteran claims.	Provide consuming business applications with access to information about the patient, their eligibility to receive care if they are authorized the care, and/or claim/billing information.	Via secure file transfer protocol within the VA network
DAPER	Administers Meds-by-Mail program	Information about the patient, their eligibility to receive care if they are authorized the care.	Via SOAP and Enterprise Cache Protocol within the VA network.
Claims XM	Used for processing veteran claims.	Eligibility data	
Office of the Inspector General (OIG)	Fraud	All, Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Provider's TIN and Address information.	Via secure file transfer protocol within the VA network, paper, and/or by phone.

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.

All data in encrypted while at rest and when transmitted electronically.
Appropriate security controls are in place to guard against unauthorized access to the data.

Follow the format below:
Privacy Risk: There is a risk that information may be shared with unauthorized VA programs or systems.

Mitigation: OIT develops, disseminates, and periodically reviews and updates access control policies and procedures. OIT has formally developed an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among other VA entities. The policies and procedures are reviewed on an annual basis by responsible parties and updated as needed.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission. This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Defense Enrollment Eligibility Reporting System (DEERS)	Information Sharing	ALL ALL-Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Provider's TIN and Address information.	23VA10NB3, 54VA10NB3	Via secure file transfer protocol within the VA network, paper, and/or by phone
Department of Defense	Information Sharing	ALL ALL-Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Health Insurance	23VA10NB3, 54VA10NB3	Outbound - Via secure file transfer protocol within the VA network

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: Only the data required to demonstrate claims status and payment is provided back to the external third-party. However, it should be noted all the data taken in comes from this same third party so in effect the only information different than the external vendor third-party's data given to us is the payment amount and canned decision reasons. PII may be accidently released to unauthorized individuals.

Mitigation: Access controls are in place at the wide area level through the NSOC gateways and firewalls. Information is only accessible to authorized individuals who gain access with their approved SSOe provided credentials and provide a password. Safeguards are implemented to ensure data is not shared with unauthorized organizations, including employee security and privacy training, 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 for the system. All users must take HIPAA and VA privacy and security training

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.

This Privacy Impact Assessment (PIA) also serves as notice of the CP&E system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." Disclosure of Social Security numbers of those for whom benefits are claimed is requested under the authority of 38 USC and is voluntary. Social Security numbers will be used

in the administration of Veterans' benefits and in the identification of Veterans or persons claiming or receiving VA benefits and their records and may be used for other purposes where authorized by 38 USC and the Privacy Act of 1974 (5 USC 552a) or where required by other statutes.

1. Beneficiaries are provided notice of privacy practices upon enrollment. A form of this notice is provided in the CHAMPVA Guide.
2. Privacy notices are provided at the point of service at the medical center where the Veteran and beneficiary receive care, in accordance with VHA Handbook 1605.4, Notice of Privacy Practices.
3. Notice of privacy practices are available on the https://www.va.gov/privacy/

Each of the above notices includes information on how to report any use of information that is not in accordance with the collection.

See Appendix A for a link to the notice of privacy practices provided at all VA medical centers.

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

Individuals do have the right to refuse to provide information but doing so may result in denial of the claim and/or inappropriate care to be provided. Yes, see **Appendix A**

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 do have the right to refuse to consent to particular uses of the information, but doing so may result in denial of the claim and/or inappropriate care to be provided.

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 VA employees will not know that Claims Processing and Eligibility collects, maintains and disseminates Personally Identifiable Information and Sensitive Personal Information.

Mitigation: Established policies within HIPAA law are followed by providers; allowing patients to be provided with a notice of claims payment purposes. Health Care information is verified by the Office of Community Care and verified per HIPAA law. Information is then sent to FMS, a payment file is created and a record is sent to the third-party provider. If notice is not provided in a timely manner, an individual might give information that they don't want to be shared.

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.

See **Appendix A** for a link to the notice of privacy practices provided at all VA medical centers, which includes the following:

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.

NOTE: Please send a written request, to your VHA health care facility Privacy Officer. 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.

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 have a right to contact the VHA call center to gain access to their information. Disclosure of Social Security numbers of those for whom benefits are claimed is requested under the authority of 38 USC and is voluntary. Social Security numbers will be used in the administration of Veterans' benefits and in the identification of Veterans or persons claiming or receiving VA benefits and their records and may be used for other purposes where authorized by 38 USC and the Privacy Act of 1974 (5 USC 552a) or where required by other statutes.

See **Appendix A** for a link to the notice of privacy practices provided at all VA medical centers, which includes the following:

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

7.3 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.

Individuals have a right to contact the VHA call center to gain access to their information. Disclosure of Social Security numbers of those for whom benefits are claimed is requested under the authority of 38 USC and is voluntary. Social Security numbers will be used in the administration of Veterans' benefits and in the identification of Veterans or persons claiming or receiving VA benefits and their records and may be used for other purposes where authorized by 38 USC and the Privacy Act of 1974 (5 USC 552a) or where required by other statutes.

See Appendix A for a link to the notice of privacy practices provided at all VA medical centers, which includes the following:

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

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 ensures data accuracy.

Individuals have a right to contact the VHA call center to gain access to their information. Disclosure of Social Security numbers of those for whom benefits are claimed is requested under the authority of 38 USC and is voluntary. Social Security numbers will be used in the administration of Veterans' benefits and in the identification of Veterans or persons claiming or receiving VA benefits and their records and may be used for other purposes where authorized by 38 USC and the Privacy Act of 1974 (5 USC 552a) or where required by other statutes.

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: If an individual discovers the VHA Office of Community Care has incorrect information on them, or an address or life event update.

Mitigation: Individuals have a right to contact the VHA call center to gain access to their information. In addition, authentication of data is in place to safeguard against incorrect information being loaded.

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.

In accordance with the SORN noted above and locally established data security procedures, access to access services information databases controlled by unique entry codes (access and verification codes). The user's verification code is automatically set to be changed every 90 days.

User access to data is controlled by role-based access as determined necessary by supervisory and information security staff as well as by management of option menus available to the employee. Determination of such access is based upon the role or position of the employee and functionality necessary to perform the employee's assigned duties.

On an annual basis, employees are required to sign a computer access agreement acknowledging their understanding of confidentiality requirements. In addition, all employees receive annual privacy awareness and information security training. Access to electronic records is deactivated when no longer required for official duties. Recurring monitors are in place to ensure compliance with nationally and locally established security measures.

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

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

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

Contractors and employees do not have any access to VA information systems and PII until they have been fully onboarded. IAM ensures screening is conducted for all contract personnel and federal employees and all other appointed workforce members. The on-boarding process consists of screening, as defined by VA Directive and Handbook 0710 Personnel Suitability and Security Program of federal employees and contract personnel who participate in the design, development, operation, or maintenance of sensitive applications and sensitive systems, as well as those individuals having access to VA sensitive information or information is required.

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.

VA has privacy and security training.

Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access

to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training.

This training includes, but is not limited to, the following TMS Courses:

- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics

Role-based Training

Includes, but is not limited to and based on the role of the user.

- VA 1016925: Information Assurance for Software Developers IT Software Developers
- VA 3193: Information Security for CIOs Executives, Senior Managers, CIOs and CFOs
- VA 1357084: Information Security Role-Based Training for Data Managers
- VA 64899: Information Security Role-Based Training for IT Project Managers
- VA 3197: Information Security Role-Based Training for IT Specialists
- VA 1357083: Information Security Role-Based Training for Network Administrators
- VA 1357076: Information Security Role-Based Training for System Administrators
- VA 3867207: Information Security Role-Based Training for System Owners

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

If Yes, provide:

1. *The Security Plan Status,* Approved
2. *The Security Plan Status Date,* July 25, 2021
3. *The Authorization Status,* Authorized
4. *The Authorization Date,* August 3, 2021
5. *The Authorization Termination Date,* August 3, 2022
6. *The Risk Review Completion Date,* July 16, 2021
7. *The FIPS 199 classification of the system* (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.***

Section 9 – Technology Usage

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

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

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

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

This system does not use cloud technology.

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

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

Not applicable.

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

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

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

Not applicable.

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

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

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

Not applicable.

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

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

Not applicable.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Michael D Hartmann 1612370

Digitally signed by Michael D Hartmann 1612370
Date: 2022.05.03 10:20:55 -06'00'

Privacy Officer, Michael Hartmann

TIMOTHY LINDSAY (Affiliate)

Digitally signed by TIMOTHY LINDSAY (Affiliate)
Date: 2022.05.03 13:08:06 -04'00'

Information Systems Security Officer, Timothy Lindsay

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2022.05.03 12:35:40 -05'00'

Information System Owner, Christopher Brown

APPENDIX A

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms):
(https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090)

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 emergencytreatment 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 facilityPrivacy 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
- The Office of the Inspector General at https://www.va.gov/oig/hotline/
- 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, limited to labs and x-rays, clinic visits, inpatient admissions
- Contacting you to provide appointment reminders 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 but not 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
- Performing process reviews and root cause analyses
- 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

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 Disease, injury, or disability
- Reporting vital events such as births and deaths
- Reporting communicable diseases, such as hepatitis, tuberculosis, sexually transmitted diseases & HIV
- Tracking FDA-regulated products
- Reporting adverse events and product defects or problems
- Enabling product recalls, repairs or replacements

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
- Investigating a specific criminal act
- 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

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 suitabilityof 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 yourbehalf.

Coroner or Funeral Services. Upon your death, we may disclose your health information to a funeraldirector 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 protectyour 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; toprotect 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 forother 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. The 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 researchbecause 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 foryou by name. Your religious affiliation will only be disclosed to members of the clergy who ask for you by name.

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 foryou 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 youreligibility 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 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).