Privacy Impact Assessment for the VA IT System called:

Claims Processing & Eligibility (CP&E)

Veterans Health Administration

Office of Integrated Veterans Care

eMASS ID #756

Date PIA submitted for review:

05/29/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Eller Pamintuan	Eller.pamintuan@va.gov	303.331.7512
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?".

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:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

Claims Processing and Eligibility (CP&E) owned by Veterans Health Administration

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

The CP&E system that is currently located in VAEC AWS West and 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.).

C. Who is the owner or control of the IT system or project?

VA Owned and VA Operated.

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?

3,185,615, affected individuals are Vets and their dependents (PII/PHI info), medical claims, birth defects, service-connected conditions.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

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 Erollment - 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. This includes the beneficiary information, vendor information and all supporting information/data required for claim processing.

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.

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. Data sharing is done to Financial Management System and Center for Medicare and Medicaid Services. Client and associated data for example accumulator data is shared with claims XM System.

G. If 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?

CP&E is a Cloud based system located in VAEC AWS West, with Disaster Recovery in VAEC AWS East. CP&E Backup is located in AWS East.

3. Legal Authority and SORN

H. What is the 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

SORN: 23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015), https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

Legal Authority: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.

SORN: 24VA10A7, Patient Medical Records - VA (10-2-2020), https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

Legal Authority: Title 38, United States Code, Sections 501(b) and 304.

43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records - VA (1/25/2021), https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01526.pdf

Legal Authority: 5 U.S.C. 306, 38 U.S.C. 527.

SORN: 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015), https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf

Legal Authority: Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101.

58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA (11/8/2021), https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

Legal Authority: Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514.

SORN: 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12-23-2020), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

Legal Authority: Title 38, United States Code, section 7301(a).

SORN: 88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8-13/2018), https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

Legal Authority: 31 U.S.C. 3101 and 31 U.S.C. 3102. The purpose of the system is consistent with the financial management provisions of title 31, United States Code, chapter 37, the pay

administration provisions of title 5, United States Code, chapter 55, and special provisions relating to VA benefits in title 38, United States Code, chapter 53.

SORN: 147VA10, Enrollment and Eligibility Records - VA (8-17-2021), https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

Legal Authority: Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.38 U.S.Code. § 501 – Veterans' Benefits Rules and Regulations

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 111–163 section 101Caregivers and Veterans' Omnibus Health Services Act of 2010- Sec. 101. Assistance and support services for caregivers.

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 § 1720G - Assistance and support services for caregivers

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

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

160—General Administrative

REQUIREMENTS

45 CFR Part 164 - Security and Privacy

4 CFR 103 - Standards for the Compromise of Claims

I. *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?*

No modifications currently being performed on the system should result in a need to amend or revise any SORN. SORNs cover cloud computing.

4. System Changes

J. *Will the completion of this PIA will result in circumstances that require changes to business processes?*

The completion of this PIA will not impact the business process.

K. *Will the completion of this PIA could potentially result in technology changes?*

The completion of this PIA will not impact the technology process

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. It must also match the information provided in question 3.4 of the PTA.

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 Information
- ☒ Health Insurance Beneficiary Numbers Account numbers

☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Current Medications
☐ Medical Records
☐ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☒ Gender
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Other Data Elements (list below)

Other PII/PHI data elements:
• Member Identification Number
• Electronic Data Interchange Personal Identified (EDIPI)
• Zip code
• Free text notes
• Patient Control Number
• Medical Record Identification Number
• Health Insurance Numbers
• Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information
• Billed Amounts
• Other Health Insurance Information
• Other Health Insurance Paid Amounts
• Provider Name
• National Provider Identifier (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, Unique Physician Identification Number (UPIN), Provider Commercial Number, Location Number)
• Health Information
• Prescription Information
• Claim Service Date
• Procedure Codes
• Procedure Date
• Images
• Location of caller

PII Mapping of Components (Servers/Database)

CP&E consists of 10 key components (6 production servers, 1 test server, 1 development server, 1 preprod server, 1 train server). 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.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**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**
Test - 1	Yes	Yes	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual)	Claims Processing	Encryption and Access is controlled

			• Health Insurance Beneficiary Numbers • Account numbers • Vehicle License Plate Number • Internet Protocol (IP) Address Numbers • Current Medications • Tax Identification Number • Medical Record Number • Gender Integrated Control Number (ICN) • Member Identification Number • Electronic Data Interchange Personal Identified (EDIPI) • Zip code • Patient Control Number • Medical Record Identification Number		

			• Health Insurance Numbers • Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information • Billed Amounts • Other Health Insurance Information • Other Health Insurance Paid Amounts • Provider Name • National Provider Identifier (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, Unique Physician Identification Number (UPIN), Provider Commercial Number, Location Number) • Health Information		
Dev - 1	Yes	Yes	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address	Claims Processing	Encryption and Access is controlled

			• Personal Phone Number(s) • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers • Account numbers • Vehicle License Plate Number • Internet Protocol (IP) Address Numbers • Current Medications • Tax Identification Number • Medical Record Number • Gender Integrated Control Number (ICN) • Member Identification Number		

			• Electronic Data Interchange Personal Identified (EDIPI) • Zip code • Patient Control Number • Medical Record Identification Number • Health Insurance Numbers • Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information • Billed Amounts • Other Health Insurance Information • Other Health Insurance Paid Amounts • Provider Name • National Provider Identifier (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, Unique Physician Identification Number (UPIN), Provider Commercial Number, Location Number)		

			• Health Information		
PreProd - 1	Yes	Yes	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers • Account numbers • Vehicle License Plate Number • Internet Protocol (IP) Address Numbers • Current Medications	Claims Processing	Encryption and Access is controlled

			• Tax Identification Number • Medical Record Number • Gender Integrated Control Number (ICN) • Member Identification Number • Electronic Data Interchange Personal Identified (EDIPI) • Zip code • Patient Control Number • Medical Record Identification Number • Health Insurance Numbers • Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information • Billed Amounts		

			• Other Health Insurance Information • Other Health Insurance Paid Amounts • Provider Name • National Provider Identifier (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, Unique Physician Identification Number (UPIN), Provider Commercial Number, Location Number) • Health Information		
Train - 1	Yes	Yes	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance	Claims Processing	Encryption and Access is controlled

			Beneficiary Numbers • Account numbers • Vehicle License Plate Number • Internet Protocol (IP) Address Numbers • Current Medications • Tax Identification Number • Medical Record Number • Gender Integrated Control Number (ICN) • Member Identification Number • Electronic Data Interchange Personal Identified (EDIPI) • Zip code • Patient Control Number • Medical Record Identification Number		

			• Health Insurance Numbers • Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information • Billed Amounts • Other Health Insurance Information • Other Health Insurance Paid Amounts • Provider Name • National Provider Identifier (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, Unique Physician Identification Number (UPIN), Provider Commercial Number, Location Number) • Health Information		
Prod - 6	Yes	Yes	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address	Claims Processing	Encryption and Access is controlled

			• Personal Phone Number(s) • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers • Account numbers • Vehicle License Plate Number • Internet Protocol (IP) Address Numbers • Current Medications • Tax Identification Number • Medical Record Number • Gender Integrated Control Number (ICN) • Member Identification Number		

			• Electronic Data Interchange Personal Identified (EDIPI) • Zip code • Patient Control Number • Medical Record Identification Number • Health Insurance Numbers • Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information • Billed Amounts • Other Health Insurance Information • Other Health Insurance Paid Amounts • Provider Name • National Provider Identifier (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, Unique Physician Identification Number (UPIN), Provider Commercial Number, Location Number)		

			• Health Information		

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a 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?
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.

1.2b 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 indicate why the system is using this source of data.

Claims Processing and Eligibility systems allows the Veteran Affairs (VA) to process claims in an efficient manner that helps enhance Civilian Health and Medical Program of the Department of Veterans Affairs (CHAMPVA) beneficiaries' access to care and expedient payment to CHAMPVA providers. This is an automated process with no system administrators/users involved.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

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?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a 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 technologies used in the storage or transmission of information in identifiable form?
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.
1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

Information is collected on form 10-10d and for application benefits 10-7959

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a 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.

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.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

CP&E does not utilize a commercial aggregator of information to operate or function, and it does not check the information for accuracy. The system has a number of commercially acquired integrity checks that automatically reject claims that do not meet HIPAA mandated requirements.

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:

SORN: 23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015), https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

Legal Authority: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.

SORN: 24VA10A7, Patient Medical Records - VA (10-2-2020), https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

Legal Authority: Title 38, United States Code, Sections 501(b) and 304.

43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records - VA (1/25/2021), https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01526.pdf

Legal Authority: 5 U.S.C. 306, 38 U.S.C. 527.

SORN: 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015), https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf

Legal Authority: Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101.

58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA (11/8/2021), https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

Legal Authority: Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514.

SORN: 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12-23-2020), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

Legal Authority: Title 38, United States Code, section 7301(a).

SORN: 88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8-13/2018), https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

Legal Authority: 31 U.S.C. 3101 and 31 U.S.C. 3102. The purpose of the system is consistent with the financial management provisions of title 31, United States Code, chapter 37, the pay administration provisions of title 5, United States Code, chapter 55, and special provisions relating to VA benefits in title 38, United States Code, chapter 53.

SORN: 147VA10, Enrollment and Eligibility Records - VA (8-17-2021), https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

Legal Authority: Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.38 U.S.Code. § 501 – Veterans' Benefits Rules and Regulations

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 111–163 section 101Caregivers and Veterans' Omnibus Health Services Act of 2010- Sec. 101. Assistance and support services for caregivers.

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 § 1720G - Assistance and support services for caregivers

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

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

160—General Administrative

REQUIREMENTS

45 CFR Part 164 - Security and Privacy

4 CFR 103 - Standards for the Compromise of Claims

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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.

Privacy Risk: The system collects, processes, and retains PII and PHI on Veterans and on Members of the Public. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.

Mitigation: Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

Privacy Risk: Data pulled by the CP&E application contains PII. If the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft might result.

Mitigation: The CP&E application ensures strict access to information by enforcing thorough access control and requirements for end users. Access to the application is by PIV authentication.

Individual administrator user IDs and access are provided based on need. The CP&E limits access rights and controls only to valid end users. There are rigorous securities monitoring controls to prevent unauthorized access and intrusion, and to protect all information. Furthermore, all end users are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. All users with access to CP&E are responsible in assuring safeguards for the PII/PHI.

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 that 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.

PII/PHI Data Element	Internal Use	External Use
Name	Used to identify the eligible beneficiary	Sent to DEERS, Signature Claims XM, Optum RX, Change Healthcare, Medicare, Austin, and Treasury
Social Security Number	Used to identify the eligible beneficiary	Sent to DEERS, Signature Claims XM, Optum RX, Change Healthcare, Medicare
Address (sponsor and beneficiary mailing, vendor remit to, and vendor billing addresses are stored as address information in CP&E database.)	1. Used to identify the eligible beneficiary and to send correspondence. 2. 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. 3.Manages the identities of individuals that access VA logical resources. 4. Authenticates users across the enterprise. 5. Authorizes/grants users' permissions to protected VA information assets. 6. Enforces access to protected VA information assets. 7. Adheres to Federal guidelines, mandates, and	* Sent to DEERS, Signature Claims XM, Optum RX, Change Healthcare, and Medicare ** Sent to Austin, and Treasury

PII/PHI Data Element	Internal Use	External Use
	timelines for information security. 8. Enables the management and oversight of auditable events and reporting for integrated services.	
Date of Birth	Captured to assist in identifying the correct sponsor or beneficiary	Sent to DEERS, Signature Claims XM, Optum RX, Change Healthcare, and Medicare
Phone Number (sponsor, beneficiary, and vendor phone numbers are stored in CP&E database.)	Capture correct contact information for the sponsor, beneficiary, and or vendor.	Sent to DEERS, Signature Claims XM, Optum RX, Change Healthcare, Medicare, Austin, and Treasury
Health Insurance Beneficiary Numbers	HICN (Health Insurance Control Number, was what was used to identify for Medicare number which is now a MBI number.	Sent to Signature Claims XM and Medicare
Free Text Notes	There are comments that are stored within database that can be placed within a sponsor's or beneficiary's file, a claim or PDI comment.	n/a
Patient Control Number	This data element is present on claim information being sent through the Electronic Data Interchange (EDI claims processing).	Trading Partners Change Healthcare.
Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information	This data will be stored within our claims database and comes in through submissions from the vendor, beneficiary, or trading partner.	Change Healthcare, FMS, and Treasury
Billed Amounts	This data will be stored within claims database and comes in through submissions from the vendors, beneficiaries, or trading partners	Change Healthcare, Optum RX, FMS and Treasury
Other Health Insurance Information	This data will be the sponsor and beneficiary database and come in through an OHI Certificate that the beneficiary completes and send in for input.	Payer EDI and Signature Claims XM
Other Health Insurance Paid Amounts	This data will be sent in on submissions received from	Change Healthcare, Optum RX, FMS and Treasury

PII/PHI Data Element	Internal Use	External Use
	vendors, beneficiaries, or trading partners and stored within our claims database.	
Provider Name	This data is stored in our vendor database.	Change Healthcare, Optum RX, FMS and Treasury
National Provider Identifier (NPI)	This data is stored in our vendor database.	Change Healthcare, Optum RX, FMS and Treasury
Provider Phone Number	This data is stored in our vendor database.	Change Healthcare, Optum RX, FMS and Treasury
Provider Billing Address	This data is stored in our vendor database.	Change Healthcare, Optum RX, FMS and Treasury
Provider Remit to Address (DoVA1)	This data is stored in our vendor database.	Change Healthcare, Optum RX, FMS and Treasury
Claim Service Date	This data element on a claim is the data of service and is store in our claims database	Change Healthcare, Optum RX, FMS, and Treasury
Procedure Codes	This information comes in through submission data for claims from vendors, beneficiaries, and trading partners and stored within our claims database.	Change Healthcare, Optum RX, FMS, and Treasury
Procedure Dates	This information comes in through submission data for claims from vendors, beneficiaries, and trading partners and stored within our claims database.	Change Healthcare, Optum RX, FMS, and Treasury

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a 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?
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.

2.2b 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.

Historical claims processed will ultimately reside in a read only state within CP&E to be utilized for data analysis and historical claims adjudication.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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?

Yes, using Vista access control. Additionally, CP&E database is encrypted at rest and SSNs are protected with SFTP.

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

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.

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.

2.4a How is access to the PII determined?

Access to PII is limited by the CP&E application to only those data items deemed necessary for an administrator to perform their job, as determined by their management team and their job description.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes, system documentation includes detailed system design and user guides that specify those areas of the system that contain PII and PHI, as well as how it is to be used by the CP&E system. Additionally, user roles are implemented to restrict user's access to only the specific information required to perform their job function. Roles within the system are determined and requested by CP&E supervisors (Senior Program Analyst or higher) or Non-VA Community Care (NVCC) Office management (Supervisors and Business Implementation Managers). User access is provided by CP&E System Administrators following receipt of request from appropriate individuals. The CP&E application implements auditing which tracks user access to the system and all data accessed. The information is mapped in the audit record by CP&E agent identifier and Veteran identifier used for data access.

2.4c Does access require manager approval?

Yes, roles within the system are determined and requested by the Information System Owner. User access is provided by the System Administrators following receipt of request from appropriate individuals.

2.4d Is access to the PII being monitored, tracked, or recorded?

The CP&E application implements auditing which tracks user access to the system and all data accessed. The information is mapped in the audit record by ~~XXXXX~~ User ID identifier and Veteran identifier used for data access.

2.4e Who is responsible for assuring safeguards for the PII?

All users of the system are responsible for assuring safeguards for the PII. The system manager is responsible for assigning users to the appropriate user roles to limit access and assuring PII safeguards as documented in the technical documentation and system design documentation. Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply.

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
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 Information
Health Insurance Beneficiary Numbers
Account numbers
Certificate/License numbers
Vehicle License Plate Number
Internet Protocol (IP) Address Numbers
Current Medications
Medical Records
Race/Ethnicity
Tax Identification Number
Medical Record Number
Gender
Integrated Control Number (ICN)
Military History/Service Connection
Next of Kin
Member Identification Number
Electronic Data Interchange Personal Identified (EDIPI)
Zip code
Free text notes
Patient Control Number
Medical Record Identification Number
Medical Record Number
Health Insurance Numbers
Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information
Billed Amounts
Other Health Insurance Information
Other Health Insurance Paid Amounts
Provider Name
National Provider Identifier (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, Unique Physician Identification Number (UPIN), Provider Commercial Number, Location Number)
Health Information
Prescription Information
Claim Service Date
Procedure Codes
Procedure Date
Images
Location of caller

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? 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. VHA Records Control Schedule (RCS) 10-1, 1260 – Care in Community, Health and Medical Care Program VA

RCS: 1260.1. Civilian Health and Medical Care (CHMC) Records.

a. Unscanned Records. All documents maintained in paper form. Temporary; destroy 6 years after all individuals in the record become ineligible for program benefits. (N1-15-03-1, item 1)

b. Input Scanned Records. Paper source documents that have been scanned for electronic media storage (optical disk). Temporary; destroy after successfully scanned to electronic medium. (N1-15-03-1, item 2)

c. Electronic Records (Master Files). Electronic records produced form scanned documents or records received electronically (optical disk, magnetic tape, or another electronic medium). Temporary; destroy 6 years after all individuals in the record become ineligible for program benefits. (N1-15-03-1, item 3)

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes. The item Number 1260.1, Care in the Community, Disposition Authority N1-15-03-1, Item 2 https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

3.3b Please indicate each records retention schedule, series, and disposition authority?

VHA Records Control Schedule (RCS) 10-1, 1260 – Care in Community, Health and Medical Care Program VA
RCS: 1260.1. Civilian Health and Medical Care (CHMC) Records.
a. Unscanned Records. All documents maintained in paper form. Temporary; destroy 6 years after all individuals in the record become ineligible for program benefits. (N1-15-03-1, item 1)
b. Input Scanned Records. Paper source documents that have been scanned for electronic media storage (optical disk). Temporary; destroy after successfully scanned to electronic medium. (N1-15-03-1, item 2)
c. Electronic Records (Master Files). Electronic records produced form scanned documents or records received electronically (optical disk, magnetic tape, or another electronic medium). Temporary; destroy 6 years after all individuals in the record become ineligible for program benefits. (N1-15-03-1, item 3)

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory 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.
Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the Deleted Items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1 and NIST SP800-88r1 as evidenced in the FedRAMP Audit reports.
The application will follow NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process of any IT storage hardware used in the application. The Guidelines establish three levels of data destruction: Clear, Purge, and Destroy, that can be applied to different data storage devices. An appropriate destruction method will be chosen based on the memory type (Flash Memory, Magnetic Drives, Optical Devices, Hard Copies etc.) used for the storage. It is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws.
Regarding temporary paper records, those that contain PII, and VA sensitive information, which are under the jurisdiction of VA, will be handled securely, economically, and effectively and disposed of properly. Written documentation that attests to the completion of the destruction

process after the final destruction is required, which could be in the form of a letter, memo, or any format attesting to its complete destruction. This certification is not considered a valid certification of destruction if completed and submitted before the final destruction of the records. The certification should contain sufficient information to attest to the final destruction of the temporary paper records – what temporary records were destroyed, the date when they were destroyed, what destruction method was used, where they were destroyed, and who was responsible for their final destruction.
Paper records are destroyed on site, destruction verification of secure shred containers is verified by the logistics department. The VHA Office of Integrated Veteran Care program office has a current shredding contract. No documents leave the facility, and system users are unable to print from a remote location.

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. 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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: 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.

Privacy Risk There is a risk that CP&E will retain information for longer than necessary which can put the records at greater risk of being breached.

Mitigation: To mitigate the risk, CP&E adheres to the retention schedule listed in RCS 10-1, where records are destroyed. The destruction procedures are outlined in 3.4

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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.	Name, Gender, Tax Identification Number (TIN), Electronic Data Interchange Personal Identifier (EDIPI), Social Security Number, Integrated Control Number (ICN), Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Email, Emergency Contact, Zip Code, Personal Phone Number(s), Location of caller, Health Insurance Beneficiary Information, Current Medications, Free Text Notes, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Health Information, Prescription Information, Claim Service Date, Procedure Codes,	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*
		Procedure Date, Images, Provider Name, National Provider Identifier (NPI), Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Email, Provider Patient Control Number, Provider Taxonomy Information, Provider Tax Identification Number (TIN), Healthcare Provider Taxonomy Code, Provider Secondary Identification, State License Number, Unique Physician, Identification Number (UPIN), Provider Commercial Number, Location Number	
Financial Management System	Used to transmit data to Treasury.	Name, Gender, Tax Identification Number (TIN), Electronic Data Interchange Personal Identifier (EDIPI), Social Security Number, Integrated Control Number (ICN), Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Email, Emergency Contact, Zip Code, Personal Phone Number(s), Location of caller, Health Insurance Beneficiary Information, Current Medications, Free Text Notes, Member Identification Number, Patient Control Number,	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*
		Medical Record Identification Number, Medical Record Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Health Information, Prescription Information, Claim Service Date, Procedure Codes, Procedure Date, Images, Provider Name, National Provider Identifier (NPI), Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Email, Provider Patient Control Number, Provider Taxonomy Information, Provider Tax Identification Number (TIN), Healthcare Provider Taxonomy Code, Provider Secondary Identification, State License Number, Unique Physician, Identification Number (UPIN), Provider Commercial Number, Location Number	
Interactive Voice Response	Self-service option to check their most	Name, Gender, Tax Identification Number (TIN), Electronic Data	Via secure file transfer protocol within the VA

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*
	recent payment information.	Interchange Personal Identifier (EDIPI), Social Security Number, Integrated Control Number (ICN), Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Email, Emergency Contact, Zip Code, Personal Phone Number(s), Location of caller, Health Insurance Beneficiary Information, Current Medications, Free Text Notes, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Health Information, Prescription Information, Claim Service Date, Procedure Codes, Procedure Date, Images, Provider Name, National Provider Identifier (NPI), Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Email, Provider	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*
		Patient Control Number, Provider Taxonomy Information, Provider Tax Identification Number (TIN), Healthcare Provider Taxonomy Code, Provider Secondary Identification, State License Number, Unique Physician, Identification Number (UPIN), Provider Commercial Number, Location Number	
VA Master Person Index (VA MPI)	The primary vehicle for assigning and maintaining unique patient identifiers.	Name, Gender, Tax Identification Number (TIN), Electronic Data Interchange Personal Identifier (EDIPI), Social Security Number, Integrated Control Number (ICN), Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Email, Emergency Contact, Zip Code, Personal Phone Number(s), Location of caller, Health Insurance Beneficiary Information, Current Medications, Free Text Notes, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded	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*
		Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Health Information, Prescription Information, Claim Service Date, Procedure Codes, Procedure Date, Images, Provider Name, National Provider Identifier (NPI), Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Email, Provider Patient Control Number, Provider Taxonomy Information, Provider Tax Identification Number (TIN), Healthcare Provider Taxonomy Code, Provider Secondary Identification, State License Number, Unique Physician, Identification Number (UPIN), Provider Commercial Number, Location Number	
Program Integrity Tool	Used for processing veteran claims.	Name, Gender, Tax Identification Number (TIN), Electronic Data Interchange Personal Identifier (EDIPI), Social Security Number, Integrated Control Number (ICN), Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Email, Emergency Contact,	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*
		Zip Code, Personal Phone Number(s), Location of caller, Health Insurance Beneficiary Information, Current Medications, Free Text Notes, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Health Information, Prescription Information, Claim Service Date, Procedure Codes, Procedure Date, Images, Provider Name, National Provider Identifier (NPI), Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Email, Provider Patient Control Number, Provider Taxonomy Information, Provider Tax Identification Number (TIN), Healthcare Provider Taxonomy Code, Provider Secondary Identification, State License Number,	

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*
		Unique Physician, Identification Number (UPIN), Provider Commercial Number, Location Number	
Veterans Affairs/Department of Defense Identity Repository (VADIR)	Information Sharing	Name, Gender, Tax Identification Number (TIN), Electronic Data Interchange Personal Identifier (EDIPI), Social Security Number, Integrated Control Number (ICN), Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Email, Emergency Contact, Zip Code, Personal Phone Number(s), Location of caller, Health Insurance Beneficiary Information, Current Medications, Free Text Notes, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Health Information, Prescription Information, Claim Service Date, Procedure Codes,	Via secure file transfer protocol within the VA network

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*
		Procedure Date, Images, Provider Name, National Provider Identifier (NPI), Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Email, Provider Patient Control Number, Provider Taxonomy Information, Provider Tax Identification Number (TIN), Healthcare Provider Taxonomy Code, Provider Secondary Identification, State License Number, Unique Physician, Identification Number (UPIN), Provider Commercial Number, Location Number	
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.	Name, Gender, Tax Identification Number (TIN), Electronic Data Interchange Personal Identifier (EDIPI), Social Security Number, Integrated Control Number (ICN), Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Email, Emergency Contact, Zip Code, Personal Phone Number(s), Location of caller, Health Insurance Beneficiary Information, Current Medications, Free Text Notes, Member Identification Number, Patient Control Number,	Via web services directly into MUMPs routines/globals

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*
		Medical Record Identification Number, Medical Record Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Health Information, Prescription Information, Claim Service Date, Procedure Codes, Procedure Date, Images, Provider Name, National Provider Identifier (NPI), Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Email, Provider Patient Control Number, Provider Taxonomy Information, Provider Tax Identification Number (TIN), Healthcare Provider Taxonomy Code, Provider Secondary Identification, State License Number, Unique Physician, Identification Number (UPIN), Provider Commercial Number, Location Number	
Veterans' Health Information System	This is the system of record for most of the claims data.	Name, Gender, Tax Identification Number (TIN), Electronic Data	Via secure file transfer protocol within the VA

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*
and Technology Architecture		Interchange Personal Identifier (EDIPI), Social Security Number, Integrated Control Number (ICN), Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Email, Emergency Contact, Zip Code, Personal Phone Number(s), Location of caller, Health Insurance Beneficiary Information, Current Medications, Free Text Notes, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Health Information, Prescription Information, Claim Service Date, Procedure Codes, Procedure Date, Images, Provider Name, National Provider Identifier (NPI), Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Email, Provider	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*
		Patient Control Number, Provider Taxonomy Information, Provider Tax Identification Number (TIN), Healthcare Provider Taxonomy Code, Provider Secondary Identification, State License Number, Unique Physician, Identification Number (UPIN), Provider Commercial Number, Location Number	
ODM	A business rules engine that supports automated decision-making for FMP claims.	Name, Gender, Tax Identification Number (TIN), Electronic Data Interchange Personal Identifier (EDIPI), Social Security Number, Integrated Control Number (ICN), Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Email, Emergency Contact, Zip Code, Personal Phone Number(s), Location of caller, Health Insurance Beneficiary Information, Current Medications, Free Text Notes, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded	Via SOAP and secure file transfer protocol within the VA network

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*
		Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Health Information, Prescription Information, Claim Service Date, Procedure Codes, Procedure Date, Images, Provider Name, National Provider Identifier (NPI), Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Email, Provider Patient Control Number, Provider Taxonomy Information, Provider Tax Identification Number (TIN), Healthcare Provider Taxonomy Code, Provider Secondary Identification, State License Number, Unique Physician, Identification Number (UPIN), Provider Commercial Number, Location Number	
My HealtheVet	Web enabled health information portal for veterans.	Name, Gender, Tax Identification Number (TIN), Electronic Data Interchange Personal Identifier (EDIPI), Social Security Number, Integrated Control Number (ICN), Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Email, Emergency Contact,	Via secure file transfer protocol within the VA network

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*
		Zip Code, Personal Phone Number(s), Location of caller, Health Insurance Beneficiary Information, Current Medications, Free Text Notes, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Health Information, Prescription Information, Claim Service Date, Procedure Codes, Procedure Date, Images, Provider Name, National Provider Identifier (NPI), Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Email, Provider Patient Control Number, Provider Taxonomy Information, Provider Tax Identification Number (TIN), Healthcare Provider Taxonomy Code, Provider Secondary Identification, State License Number,	

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*
		Unique Physician, Identification Number (UPIN), Provider Commercial Number, Location Number	
PED Cloud	Used for processing veteran claims.	Name, Gender, Tax Identification Number (TIN), Electronic Data Interchange Personal Identifier (EDIPI), Social Security Number, Integrated Control Number (ICN), Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Email, Emergency Contact, Zip Code, Personal Phone Number(s), Location of caller, Health Insurance Beneficiary Information, Current Medications, Free Text Notes, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Health Information, Prescription Information, Claim Service Date, Procedure Codes,	Via secure file transfer protocol within the VA network

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*
		Procedure Date, Images, Provider Name, National Provider Identifier (NPI), Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Email, Provider Patient Control Number, Provider Taxonomy Information, Provider Tax Identification Number (TIN), Healthcare Provider Taxonomy Code, Provider Secondary Identification, State License Number, Unique Physician, Identification Number (UPIN), Provider Commercial Number, Location Number	
DAPER	Administers Meds-by-Mail program	Name, Gender, Tax Identification Number (TIN), Electronic Data Interchange Personal Identifier (EDIPI), Social Security Number, Integrated Control Number (ICN), Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Email, Emergency Contact, Zip Code, Personal Phone Number(s), Location of caller, Health Insurance Beneficiary Information, Current Medications, Free Text Notes, Member Identification Number, Patient Control Number,	Via SOAP and IRIS within the VA network.

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*
		Medical Record Identification Number, Medical Record Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Health Information, Prescription Information, Claim Service Date, Procedure Codes, Procedure Date, Images, Provider Name, National Provider Identifier (NPI), Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Email, Provider Patient Control Number, Provider Taxonomy Information, Provider Tax Identification Number (TIN), Healthcare Provider Taxonomy Code, Provider Secondary Identification, State License Number, Unique Physician, Identification Number (UPIN), Provider Commercial Number, Location Number	

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: 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.

Privacy Risk: Disclosure of information from a third party

Mitigation: An Interconnection Security Agreement / Memorandum of Understanding (ISA/MOU) defining the system and data transmission is in place. Access to the data is limited to appropriate personnel who are required to be trained in the handling of VA PII/PHI and sensitive information.

Privacy Risk: Privacy information may be inadvertently released to unauthorized individuals or the VistA source applications (i.e., E&E, HDR, MPI, and CP&E) with which the application interfaces with may inadvertently release privacy information. If such an instance should occur the impact is considered low.

Mitigation: The application ensures strict access to information by enforcing through access control and requirements for end users. Access to the application is by PIV authentication. Individual administrator user IDs and access are provided only based on need. The application limits access rights and controls only to valid end users. Rigorous security monitoring controls are in place to prevent unauthorized access and intrusion, and to protect all information. Furthermore, all end users are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. The VA IT office is responsible in assuring safeguards for the PII

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***
n/a	***n/a***	***n/a***	***n/a***	***n/a***

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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (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?

These questions are 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.

6.1a 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, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

It is Veterans Health Administration (VHA) policy that the VHA Notice of Privacy Practices (Information Bulletin 10-163) is created, maintained, and distributed in compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule at 45 C.F.R. § 164.520, to inform Veterans, beneficiaries, caregivers, and non-Veteran patients of the use and disclosure of their health information without authorization, their rights to access and restrictions

on certain uses and disclosures and VHA's legal duties to maintain the privacy of their health information. AUTHORITY: 45 C.F.R. parts 160 and 164. VHA Notice of Privacy Practice

https://www.va.gov/files/2022-10/10-163p_%28004%29_-Notices_of_Privacy_Practices-_PRINT_ONLY.pdf

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

N/A

6.1c 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.

System of Record Notices (SORNs) - The Privacy Act requires agencies to "publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records" subject to the Act (5 U.S.C. 552a(e)(4)).

SORN: 23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015), https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

SORN: 24VA10A7, Patient Medical Records - VA (10-2-2020), https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records - VA (1/25/2021), https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01526.pdf

SORN: 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015), https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf

58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA (11/8/2021), https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

SORN: 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12-23-2020), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

SORN: 88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8-13/2018), https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

SORN: 147VA10, Enrollment and Eligibility Records - VA (8-17-2021), https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

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.

VHA Directive 1605.1, Privacy and Release of Information, paragraph 5, lists the Individuals' Rights of the Veterans and Beneficiaries to request VHA to restrict the use and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. Veterans have the right to refuse to disclose their SSNs to VHA. The individual is denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (please refer to the: 38 Code of Federal Regulations CFR 1.575(a)).
If the Veterans or Beneficiaries does not wish to provide their SSN, they may provide their EDIPI. Alternatively, they may provide their First Name, Last Name, and Date of Birth. If the stakeholder does not wish to provide any of this information, there is no denial of service; however, the employee will be unable to assist the stakeholder

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

VHA Handbook 1605.1, Privacy and Release of Information, paragraph 5 lists the Individuals' rights of Veterans and Beneficiaries to request VHA to restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record.

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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.**

Privacy Risk: If employees do not provide notice to stakeholders, then they will not know how the information they provide to the application is being used. The magnitude of impact is low if Veterans and Beneficiaries are not provided this notice because the employees are not collecting new data. The employees are merely verifying authoritative data stored in CP&E.

Mitigation: Contractor and VA employees are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. In addition, this PIA, which will be available online as required by the eGovernment Act of 2002, Pub. L. 107–347§208(b)(1)(B)(iii), serves to notify Veterans, Beneficiaries and Providers about the collection and storage of personal information.

Privacy Risk: Privacy Information is used or disclosed outside of its intended purpose.

Mitigation: This PIA serves to notify Veterans and Beneficiaries about the collection and storage of personal information.
1.Beneficiaries are provided notice of Privacy Practices upon enrollment.
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 VA's website at https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a 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.

VHA Directive 1605.01: Privacy and Release of Information states the rights of Veterans and Beneficiaries to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review or seek copies of records must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access to data must be delivered to, and reviewed by, the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must include the signature of the requester, date of birth, copy of signed government identification, state what is request and the period of the information requested. Mail requests for eligibility information/records to: CHAMPVA Eligibility PO Box 469028 Denver, CO 80246-9028. Mail requests for CHAMPVA billing/claim records to: VHA Office of Integrated Veteran Care Privacy/FOIA Office, PO Box 469060 Denver, CO 80246-9060. Requests for medical and pharmacy records contact your servicing medical provider and for Community Care authorizations/authorization numbers are located at the referring VA Medical Center. For Veteran claim payment information will need to be submitted to the VA Financial Services Center (FSC) Privacy Office by first contacting them via email at vafscprivacyofficer@va.gov for secure submission methods. For Veteran Explanation of Benefits maintained by the VA's Third-Party Administrators may be requested by the Veteran registering and requesting their records from either (TriWest Healthcare Alliance) (https://veteran.triwest.com/bizflowappdev/apps/veteranportal/?tz=GMT-0700 or Optum (https://veteran.vacommunitycare.com/start). Medical and pharmacy records should be sought from the medical facility where the patient received care.and Veteran and Beneficiary (CHAMPVA) lien or subrogation requests should be submitted to the respective action office via the instructions located at https://www.va.gov/OGC/Collections.asp.

7.1b 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)?

The system does not collect information from individuals. The Sources collecting the information provide this notice. Individuals have the rights to request access to review their records by submitting the VHA-10-5345 provides the process to Request for and Authorization to Release Medical Records or Health Information.

7.1c 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?

The system does not collect information from individuals. The Sources collecting the information provide this notice. Individuals have the rights to request access to review their records by submitting the VHA-10-5345 provides the process to Request for and Authorization to Release Medical Records or Health Information

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.

Veterans and beneficiaries have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request must be mailed or delivered to the organization that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

Individuals have the right to request an amendment (or correction) to information in the system records if they believe it is incomplete, inaccurate, untimely, or unrelated to operations. If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes those previously provided.

VHA Handbook 1605.1, paragraph 5 lists the rights of Veterans and Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans and beneficiaries may request changes to their information in accordance with VHA Handbook 1605.1, paragraph 5 states the rights of veterans and beneficiaries to amend their records by submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, which may be used as the written request requirement. This includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.57

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

If a Veteran or Beneficiary discovers that incorrect information was provided during the intake process, they must submit an information amendment request. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579

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.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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.

Privacy Risk: There is a risk that incorrect information is accidentally recorded in an individual's record. An individual may want to review the content of their record to check for data accuracy. The magnitude of harm associated with this risk to the VA is low.

Mitigation: An individual who wishes to determine whether a record is being maintained in this system under their name or other personal identifier, or who wants to review the contents of such a record, should submit a written request. Inquiries should include the patient's full name, SSN, and return address.

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?

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.

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

The supervisor/Contracting Officer's Representative (COR) documents and monitors individual information system security training activities, including basic security awareness training and specific information system security training. This documentation and monitoring is performed through the use of the Talent Management System (TMS). Access to the system is granted to VA employees and contractors the supporting IT for the application after the supervisor/COR authorizes this access once requirements have been met. Only the IT system administrators authorized by VA IT will have the security role to modify the application. This PIA will not result in technology protocol changes, additional controls, or single sign on, as per privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1b 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?

Access to the Payer CP&E system is limited to authorized users – VA staff who have completed the required training and agreed to rule of behavior will have view only access on a need-to-know basis. All user accounts allow read only access to data. All users must be VA cleared.

8.1c 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.

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. Contractors must go through background checks, sign the rules of behavior, and have the same restrictions as VA staff. The 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. The Office of Integrated Veterans Care (IVC) is responsible for ensuring that all contractors who are working on IVC projects have signed Business Associate Agreement and meet any necessary contractual requirements governing access and handling of Veteran data.

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

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

Personnel 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?

8.4a If Yes, provide:

1. *The Security Plan Status: Approved*
2. *The System Security Plan Status Date: 07/05/2023*
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 07/06/2024
5. *The Authorization Termination Date:* 07/06/2024
6. *The Risk Review Completion Date:* 07/05/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* (HIGH)

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

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

<<ADD ANSWER HERE>>

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), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). 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**. (Refer to question 3.3.1 of the PTA)*

CP&E is hosted in VAEC AWS.

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). (*Refer to question 3.3.2 of the PTA) 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**

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

Signature of Responsible Officials

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

ELLER PAMINTUAN

Digitally signed by ELLER PAMINTUAN
Date: 2024.08.28 14:18:34 -06'00'

Privacy Officer, Eller Pamintuan

TIMOTHY LINDSAY (Affiliate)

Digitally signed by TIMOTHY LINDSAY (Affiliate)
Date: 2024.09.17 15:53:58 -04'00'

Information System Security Officer, Timothy Lindsay

CHRISTOPHER BROWN

Digitally signed by CHRISTOPHER BROWN
Date: 2024.09.16 10:07:41 -05'00'

Information System Owner, Christopher Brown

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; screen shot of a website collection privacy notice).

(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 copayments. Therefore, this provision does not apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of your health information to a health plan for the purpose of receiving payment for health care services VA provided to you.

To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests

to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. If we agree to your request, we will honor the restriction until you revoke it unless the information covered by the restriction is needed to provide you with emergency treatment or the restriction is terminated by VHA upon notification to you.

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

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

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

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

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

• The Privacy Officer at your local VHA health care facility. Visit this Web site for VHA facilities and telephone numbers http://www.va.gov/directory/guide/home.asp?isflash=1

• VA via the Internet through "Contact the VA" at http://www.va.gov or by dialing 1-800-983-0936 or by writing the VHA Privacy Office (10A7) at 810 Vermont Avenue NW, Washington, DC 20420.

• The U.S. Department of Health and Human Services, Office for Civil Rights at http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

• 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, • Filling and submitting prescriptions but not limited to labs and x-rays, clinic visits, inpatient for medications, supplies, and equipment

admissions • Coordination of care, including care from

• Contacting you to provide appointment reminders non-VHA providers

about treatment alternatives • Communicating with non-VHA providers

• Seeking placement in community living centers or regarding your care through health

skilled nursing homes information exchanges

• Providing or obtaining home-based services or • Coordination of care with DoD, including

hospice services 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 • Pre-certifying insurance benefits

• Paying for non-VHA care and services, including • Billing and collecting for health care services

but not limited to, CHAMPVA, Choice and fee basis provided by VHA

• Coordinating benefits with other insurance payers • Reporting to consumer reporting agencies

• Finding or verifying coverage under a health insurance regarding delinquent debt owed to VHA.

plan or policy

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 • Conducting health care training • Legal services

services programs • Conducting accreditation

• Conducting Veteran and • Managing, budgeting and activities

beneficiary satisfaction surveys planning activities and reports

• Reviewing competence or • Improving health care processes, • Certifying, licensing, or qualifications of health care reducing health care costs and credentialing of health care professionals assessing organizational performance professionals

• Providing information about • Developing, maintaining and • Conducting audits and treatment alternatives or other supporting computer systems compliance programs, including health-related benefits and •Addressing patient complaints fraud, waste and abuse services investigations

• Performing process reviews

and root cause analyses

Examples:

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

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

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

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

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

Serious and Imminent Threat to Health and Safety. We may use or disclose your health information without your authorization when necessary to prevent or lessen a serious and imminent threat to the health and safety of the public, yourself, or another person. Any disclosure would only be to someone able to help prevent or lessen the harm, such as a law enforcement

agency or the person threatened. You will be notified in writing if any such disclosure has been made by a VHA health care facility.

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

• Controlling and preventing • Reporting communicable diseases, • Reporting adverse events

Disease, injury, or disability such as hepatitis, tuberculosis, sexually and product defects or problems

• Reporting vital events such transmitted diseases & HIV • Enabling product recalls,

as births and deaths • Tracking FDA-regulated products 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 • Routine reporting to law enforcement

has admitted to participating in a violent crime agencies, such as gunshot wounds

• Reporting a death where there is a suspicion that • Providing certain information to identify or death has occurred as a result of a crime locate a suspect, fugitive, material witness, or

• Reporting Fugitive Felons missing person

• Investigating a specific criminal act

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

Cadaveric Organ, Eye, or Tissue Donation. When you are an organ donor and death is imminent, we may use or disclose your relevant health information without your authorization to an Organ

Procurement Organization (OPO), or other entity designated by the OPO, for determining suitability of your organs or tissues for organ donation. If you have not specified your donation preferences and can no longer do so, your family may make the determination regarding organ donation on your behalf.

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

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

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

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

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

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

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

•A researcher is preparing a plan for a research project. For example, a researcher needs to examine patient medical records to identify patients with specific medical needs. The researcher must agree to use this information only to prepare a plan for a research study; the researcher may not use it to contact you or actually conduct the study. 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 research because privacy and confidentiality risks are minimal and other regulatory criteria are satisfied.

•A Limited Data Set containing only indirectly identifiable health information (such as dates, unique characteristics, unique numbers or zip codes) is used or disclosed, with a data use agreement (DUA) in place.

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

Example:

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

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

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

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

•Verification of identity

•Your condition described in general terms (e.g., critical, stable, good, prognosis poor)

•Your location in a VHA health care facility (e.g., building, floor, or room number)

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

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

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

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

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

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

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

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

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

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

When We Will Not Use or Disclose Your Health Information

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

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

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

Contact Information: You may 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).

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices