Privacy Impact Assessment for the VA IT System called:

Community Care Referral and Authorization (CCRA) Software as a Service (SaaS) and Integration Development

Veteran Health Administration (VHA) Integrated Veteran Care (IVC)

Date PIA submitted for review:

July 1, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michael Hartmann	michael.hartmann@va.gov	303-780-4753

	Name	E-mail	Phone Number
Information System Security Officer (ISSO)	Kimberly Keene	kimberly.keene@va.gov	703-411-3063
Information System Owner (ISO)	Chris Brown	christopher.brown1@va.gov	202-270-1432

Abstract

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

The Community Care Referral and Authorization (CCRA) Software as a Service (SaaS) and Integration Development solution is an enterprise-wide system used by community care staff to automatically generate referrals and authorizations for all Veterans receiving care in the community. CCRA allows Veterans Health Administration (VHA) and non-VA clinical providers to access a cloud-based software system and request and refer clinical care for Veterans with non-VA community care providers. The system provides many automated workflow solutions, is designed to track Veterans' wait times for community care and allows appointment scheduling. It tracks and retain health care information and correspondence necessary for Veterans to be seen for appropriate and approved episodes of care. The exchange of health care information and authorizations has enhanced VHA's ability to ensure that Veterans receive the best health care available to address their medical needs. HealthShare Referral Manager (HSRM) is listed in the technical reference model (TRM) and was approved (with constraints) on June 2, 2017.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*

- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Information Technology (IT) system name is HSRM, and it is owned by the VHA Integrated Veteran Care (IVC). The solution has enabled the scheduling of appointments with community care providers and tracks Veterans' wait times for community care.

CCRA is utilizing a SaaS solution, HSRM, hosted in an Amazon Web Services (AWS) Government Cloud (GovCloud) authorized under the Federal Risk and Authorization Management Program (FedRAMP) at the high-impact level. Community care staff members use HSRM to generate referrals and authorizations for episodes of care to community providers within the Community Care Network (CCN). The CCRA solution is an integral component of the U.S. Department of Veterans Affairs (VA) community care IT architecture that allows Veterans to receive care from health care providers in the community.

The affected individuals are Veterans who are referred by VA to community providers for medical treatment. CCRA allows these providers to view relevant patient and clinical information from Veterans Health Information Systems and Technology Architecture (VistA), Cerner, Standardized Episode of Care (SEOC) / One Consult, Enrollment System (ES), and Master Patient Index (MPI) via application program interfaces. The number of affected individuals is estimated to be over 3.25 million with an anticipated Coordinated Access and Rewarding Experiences expansion.

CCRA allows VA and non-VA clinical providers to access a cloud-based software system and request and refer clinical care for Veterans with community care providers. The system provides automated workflow solutions, enables the scheduling of appointments with community care providers, and tracks Veterans' wait times for community care. It tracks and retain the health care information and correspondence necessary for Veterans to be seen for appropriate and approved episodes of community care. The exchange of health care information and authorizations enhances VA's ability to ensure that Veterans receive the best health care available to address their medical needs.

The CCRA solution is an enterprise-wide system used by community care staff to automatically generate referrals and authorizations for all Veterans receiving care in the community. Clinical and VA community care staff located at VA medical centers (VAMCs), outpatient clinics, community-based outpatient clinics (CBOCs), and Veterans Integrated Service Network (VISN) offices use this solution. The CCRA solution is an integral component of the VA community care IT architecture that allows Veterans to receive care from community providers in all five regions.

The Emergency Care Reporting (ECR) tool facilitates emergency care payments. The modernized version of ECR, hosted within the AWS GovCloud, supports direct entry of emergency care notifications through the newly designed portal. This enhancement empowers automation in order to minimize administrative burdens, presents a unified architecture allowing for simplicity of sustainment and further modernization over time, and integrates with systems like various financial

systems. Similar to VistA, ECR is treated as a source of emergency care notification data for VA. VA adjudicates emergency care notifications for VA's vast, nationwide network of Veterans.

The Veterans Access, Choice, and Accountability Act of 2014 (VACAA) (Public Law 113-146) Section 101 requires VA to improve Veterans' access to health care by allowing eligible Veterans to use eligible health care providers outside the VA system. To comply with this act, solutions such as CCRA are needed to improve and expand the availability of medical services provided to Veterans. VA has legal authority to share information that falls under 38 United States Code (U.S.C.) 8111 and 10 U.S.C. 1104 for Military Treatment Facilities; Indian Health Services 25 U.S.C. Sections 1645, 1647; 38 U.S.C. Sections 523(a), 6301-6307, 8153; and academic sharing agreements 38 U.S.C. 8153. The legal authorities covering CCRA use of protected health information (PHI) and PII for medical care are Public Law 115-26, Public Law 104-191, and 45 Code of Federal Regulations (C.F.R.) 164.506. The CCRA system implements process changes to meet the requirements of Veterans Access, Choice, and Accountability Action (VACAA) (Public Law 113-146) Section 101. The CCRA system leverages data from VistA, Cerner, MPI, Provider Profile Management System (PPMS), SEOC/One Consult, and ECR; no changes to other systems or technologies are anticipated. No amendment of the current system of records notices is required. Information in this system is collected, maintained, and disclosed in accordance with 23VA10BN3, 24VA10P2, 121VA10P2, 147VA10BF1, 79VA10P2, 97VA10P1 and 180VA10D.

The CCRA system is hosted in an AWS GovCloud virtual private cloud; AWS GovCloud was first authorized under FedRAMP at the high-impact level in June 2016, with two subsequent expansions of that authorization in 2017, including additional AWS services within the scope of the FedRAMP authorization. CCRA is planned for enterprise integration to a number of VA systems, both inside and outside community care. HealthShare is listed in the TRM and was approved (with constraints) on June 2, 2017. VA is the owner of the data; data rights are an explicit part of the contractual agreements between VA and the Cognosante operating CCRA. Security for data stored within or processed by CCRA is a responsibility shared among AWS, VA, and the CCRA contractor, as described at a high level in AWS' shared responsibility model documentation and incorporated by reference in terms of service for customers of AWS cloud computing services.

The contractor's responsibility for safeguarding the security and privacy of VA data is explicit in VA Handbook 6500.2. The contractor shall notify the VA Security Officer within 24-hours of the discovery or disclosure of successful exploits of the vulnerability that can compromise the security of the systems (including the confidentiality or integrity of its data and operations or the availability of the system). Such issues will be remediated as quickly as is practical, but in no event longer than one calendar day. When the security fixes involve installing third-party patches (such as patches to Microsoft operating system or Adobe Acrobat), the contractor will, within 10 working days, provide written notice to VA that the patch has been validated as not affecting the systems. When the contractor is responsible for operations or maintenance of the systems, the security fixes will be applied within one calendar day. The data stored within and processed by CCRA includes PHI and PII, information types to which VA has assigned a high security categorization under Federal Information Processing Standard (FIPS) Publication 199 guidelines, indicating the potential for high impact if such data is disclosed to unauthorized parties.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

- Residential Address

- Electronic Data Interchange Personal Identifier (EDIPI)
- Data File Number (DFN)
- Gender
- Beneficiary Type (whether the individual is a Veteran or spouse of a Veteran)
- Contact Notes (additional information regarding contacting the patient)
- Preferred Contact Method
- Preferred Language
- Translator Required
- Veterans Choice Eligibility
- Service-Connected Disability
- Provider Demographics
- Appointment Information
- Community Provider Information
- Program Authority
- Religion
- Provisional Diagnosis
- Category of Care
- Services Requested

PII Mapping of Components

CCRA SaaS and Integration Development consists of zero key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CCRA SaaS and Integration Development and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A	N/A	N/A	N/A	N/A	N/A

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

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

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

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

CCRA SaaS and Integration Development receives data from VA systems which gather the data. No data is collected from an individual or veteran directly. Those VA system include PPMS, VistA, Cerner, MPI, SEOC/One Consult, and ES.

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

CCRA SaaS and Integration Development receives data from VA system which gather the data. No data is collected from an individual or veteran directly. All information is delivered to CCRA electronically using various forms of technology, including Health Level 7 (HL7) messaging, JavaScript Object Notation (JSON), and extensible markup language (XML) over REST(ful) and Simple Object Access Protocol (SOAP).

VA systems provide source data, which are either transmitted via VA network or VA employee verified and entered. Those VA systems include PPMS, VistA, Cerner, MPI, SEOC/One Consult, and ES.

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

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that

receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

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

Data received and maintained by this system checked against any other source of information (within IVC) before the information is received or used to make decisions about an individual. Data that cannot be automatically verified through VA network connections are VA employee verified utilizing data within VA systems instead of CCRA.

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

The legal authorities covering the CCRA use of PHI and PII for medical care are as follows:

- VACAA (Public Law 113–146)
- Amendment to VACAA (Public Law 115-26)
- Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191)
- Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations (45 C.F.R. 164.506)
- 38 U.S.C. Coordination and Promotion of Other Programs Affecting Veterans and Their Dependents, Sections 523(a), 6301-6307, section 7301(a) 8111, 8153
- 10 U.S.C. 1104, Sharing of Health Care Resources with the Department of Veterans Affairs
- 26 U.S.C. Internal Revenue Code, 61, Gross Income Defined
- 26 U.S.C. 31, Employment Taxes and Collection of Income Tax at Source
- 26 U.S.C. 1741–1743 Criteria for Payment
- 28 U.S.C. 1781, Transmittal of Letter Rogatory or Request
- 42 U.S.C. 1786, Special Supplemental Nutrition.
- 8 U.S.C. 1787 – Health Care of Family Members of Veterans
- 38 U.S.C. 3102, Basic Entitlement
- 38bnhv, U.S.C. 5701 Confidential Nature of Claims
- 5 U.S.C. Travel and Transportation Expenses of Employees Transferred; Advancement of Funds; Reimbursement on Commuted Basis
- 38 U.S.C. 7332 Confidentiality of Certain Medical Records
- 18 U.S.C. 8131–8137, Economic Espionage, 8 Code of Federal Regulations 2.6
- 45 C.F.R. Part 160 and 164, Emergency Board

- Title 44 U.S.C. Public Printing and Documents
- Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014
- Title 38 U.S.C. 7301(a); Title 38 United States Code 1703 – Veterans Community Care Program; Veterans Access, Choice, and Accountability Act of 2014 (Pub. L. 113–146).
- Title 38, U.S.C. Sections 501(a), Rules and Regulations 1705, Management of Health Care: Patient Enrollment System, 1710, Eligibility for Hospital, Nursing Home, and Domiciliary Care, 1722, Determination of Inability to Defray Necessary Expenses; Income Thresholds, 1722(a), Determination of Inability to Defray Necessary Expenses; Income Thresholds, 1781, Medical Care for Survivors and Dependents of Certain Veterans
- Title 5, U.S.C. Section 552(a), Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings
- Title 38 U.S.C. 7301(a), Title 38 U.S.C. 1703 – Veterans Community Care Program; Veterans Access, Choice, and Accountability Act of 2014 (Pub. L. 113–146).

System of Record Notice (SORN) routine use Title 44 U.S.C. Applicable SORNs include:

- 23VA10NB3, Non-VA Care (Fee) Records-VA, published July 30, 2015
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA, published March 3, 2015
- 155VA10NB, Customer Relationship Management System (CRMS) – VA published March 3, 2015
- 180VA10D, HealthShare Referral Manager (HSRM) – VA, published August 17, 2021

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:
Privacy Risk: CCRA SaaS and Integration Development contains Sensitive Personal Information (SPI), including SSNs, names, and PHI. Due to the nature of this data, there is a risk that if the data were accessed by an unauthorized individual, or otherwise breached, identity theft or other serious harm could occur.

Mitigation: CCRA SaaS and Integration Development is utilizing a SaaS solution (HSRM) hosted in an AWS GovCloud authorized under FedRAMP at the high-impact level. The system is monitored for unusual activity using automated and manual tools, and abnormal activity is immediately addressed.

Section 2. Uses of the Information

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

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

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

The information collected or maintained by CCRA SaaS and Integration Development includes:

- Name: Used to identify the Veteran.
- SSN: Used to identify the Veteran.
- DOB: Used to determine the Veteran's age, inform community care providers, and to support medical treatment and decision-making.
- Residential Address: Used to determine nearest community provider for care.
- Mailing Address: Used to facilitate communication.
- Zip Code: Used as part of the mailing address to facilitate communication.
- Phone Number(s): Used to facilitate communication.
- Race/Ethnicity: Used to inform community providers, support medical treatment, and decision making.
- ICN: Used to identify the Veteran.
- DFN: Used to identify the Veteran.
- EDIPI: Used to identify the Veteran.
- Gender: Used to inform community providers, support medical treatment, and decision making.
- Contact Notes: Used to facilitate communication.
- Preferred Contact Method: Used to facilitate communication.
- Preferred Language: Used to information community providers and facilitate communication.
- Translator Required: Used to information community providers and facilitate

communication.

- Veterans Eligibility: Used to indicate approval for a Veteran to receive specific medical care by a community care provider and ensure VA will pay for the authorized non-VA services.
- Other Health Information: Used to inform Revenue if they care recoup funds from other health insurers.
- Provider Demographics: Used to identify and locate providers.
- SEOC: Used to informs the services authorized on the referral.

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

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

HSRM uses built-in reporting tools to analyze data. This tool is used for aggregation and filtering, and statistical reports and not for novel findings. HSRM allows community providers to upload documents containing any data that they choose. These documents are subsequently moved to more appropriate locations (such as VistA imaging) via a task assignment processes.

The CCRA SaaS and Integration Development solution utilizes Splunk to determine in an automated way if any abnormal activity occurs within the system. Additionally, periodic review of certain audit logs is conducted manually, as documented in the quarterly reports.

2.3 How is the information in the system secured?

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

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

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

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

HRSM data is encrypted at rest and in transit. SSNs are encrypted and masked via the HSRM application interface and other PII/PHI details are protected based on access to the application and the "need to know" basis.

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

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

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

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

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

Access to PII is limited by role assignment, which is completed in one of two ways:

- Option 1: Roles are assigned via the same user process and list as provisioning below, where roles can be provided and loaded into the system.
- Option 2: A manual process is employed via a help desk call with the same process and caveats as above, local IT for SSOi and for SSOe.
-

Criteria, procedures, controls, and responsibilities are enumerated in the CCRA SaaS and Integration Development End User Secure Access Management Plan. Access requires manager approval. The Cognosante IT Service Desk receives communications from the end user staff management to create an account via the Cognosante ticketing process. The request is initiated by the user's direct supervisor and approved by the project's Operations Manager for HSRM. The email contains the position requirements and role of the end user, which outlines the user's hire date and role specifications. Upon notification from the applicable trainer that the user has successfully completed the HIPAA/security awareness, privacy and security, and compliance training, the Service Desk creates the user's account, including username, role, and dashboard, in accordance with Cognosante Access Control Policies and Procedures. Access to PII/PHI is monitored using automated tools, including Alert Logic; alerts are generated automatically. The contractor's responsibility for safeguarding the security and privacy of VA data is explicit in the

contract executed between the contractor and the government.

Section 3. Retention of Information

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

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system.
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

The information collected or maintained by CCRA SaaS and Integration Development includes Name, SSN, DOB, Mailing Address, Zip Code, Phone Number(s), Information Health Insurance (Beneficiary Numbers, Account Numbers), Race/Ethnicity, EDIPI, Gender, Beneficiary Type (whether the individual is a Veteran or spouse of a Veteran), Contact Notes (additional information regarding contacting the patient), Preauthorization, Preferred Contact Method, Preferred Language, Translator Required, Veterans Choice Eligibility, and Service-Connected Disability, Emergency Contact, Current Medications, Previous Medical Record, Race/Ethnicity, and Provider Demographics.

3.2 How long is information retained?

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

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

CCRA SaaS and Integration Development relies on information in VistA, Cerner, AWS GovCloud, and MPI and only collects information related to referrals. All data is retained as part of the individual's health care record and is retained according to the rules applied to those records.

Referrals begin at the VAMC (which the original would be maintained in the VAMC Medical Files (75 years after last episode of care) then go the CCRA (these records are working records (temporary 3 years after last episode of care). At the conclusion of care, the records are returned to the VAMC (which the original would be maintained in the VAMC Medical Files) (75 years after last episode of care).

Patient appointment and appointment schedules records shall be maintained per Records Control Schedule (RCS) 10–1 item; 2201.1. According to General Records Schedule (GRS) 5.1 item 010, DAA–GRS–2017– 0003–0001, temporary destroy transitory records, messages coordinating schedules, appointments, and events when no longer needed for business use, or according to agency predetermined time or business rule.

6000.1. Health Records Folder File or CHR (Consolidated Health Record).
This records series contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system.

a. Health Records Folder. This file constitutes the active medical or clinical records segment of the CHR. It completely documents diagnostic examinations and definitive medical, surgical, psychiatric, and dental care or treatment rendered a patient at a VA health care facility or at VA expense. It contains, in written and graphic form, the diagnostic; treatment and sociological information compiled by various members of the medical care team who participated in the care of a patient during one or more courses of treatment. In addition, it is intended to meet the legal, administrative, teaching and research needs of the VA medical staff, and provides a means of studying and evaluating the type of care rendered. VA and other monetary benefits are sometimes decided by use of information from the Health Records Folder.

   Temporary; retain in VA health care facility until 3 years after last episode of care, and then convert to an inactive medical record. (N1-15-91-6, Item 1a)

b. Outpatient Treatment Folders currently on hand at VA medical facilities.

   Temporary; transfer to Health Record File or CHR and retain in VA health care facility until 3 years after last episode of care, then convert to a Perpetual Medical Record and an Inactive Medical Record. (NI-15-87-4, Item 4a)

The information retained by the CCRA system is listed in Section 3.1. (This information pertains only to records that are maintained in the CCRA system.) Feeder records are original records and are maintained in accordance with VistA, Cerner, AWS GovCloud and MPI records retention policy and the VistA, Cerner, and MPI PIA documents.

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

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

Yes, VA RCS 10-1, https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

Patient appointment and appointment schedules records shall be maintained per RCS 10–1 item; 2201.1. According to GRS 5.1 item 010, DAA–GRS–2017– 0003–0001, temporary destroy transitory records, messages coordinating schedules, appointments, and events when no longer needed for business use, or according to agency predetermined time or business rule.

6000.1. Health Records Folder File or CHR.
This records series contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system.

a. Health Records Folder. This file constitutes the active medical or clinical records segment of the Consolidated Health Record. It completely documents diagnostic examinations and definitive medical, surgical, psychiatric, and dental care or treatment rendered a patient at a VA health care facility or at VA expense. It contains, in written and graphic form, the diagnostic; treatment and sociological information compiled by various members of the medical care team who participated in the care of a patient during one or more courses of treatment. In addition, it is intended to meet the legal, administrative, teaching and research needs of the VA medical staff, and provides a means of studying and evaluating the type of care rendered. VA and other monetary benefits are sometimes decided by use of information from the Health Records Folder.

   Temporary; retain in VA health care facility until 3 years after last episode of care, and then convert to an inactive medical record. (N1-15-91-6, Item 1a)

b. Outpatient Treatment Folders currently on hand at VA medical facilities.

   Temporary; transfer to Health Record File or CHR and retain in VA health care facility until 3 years after last episode of care, then convert to a Perpetual Medical Record and an Inactive Medical Record. (NI-15-87-4, Item 4a)

NARA Link: https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.?
This question is related to privacy control DM-2, Data Retention and Disposal

CCRA SaaS and Integration Development relies on information in VistA, Cerner, AWS GovCloud, and MPI and only collects information related to referrals. All data is retained as part of the individual's health care record and is retained according to the rules applied to those records.

Referrals begin at the VAMC (which the original would be maintained in the VAMC Medical Files (75 years after last episode of care) then go the CCRA (these records are working records (temporary 3 years after last episode of care). At the conclusion of care, the records are returned

to the VAMC (which the original would be maintained in the VAMC Medical Files) (75 years after last episode of care).

Patient appointment and appointment schedules records shall be maintained per Records Control Schedule (RCS) 10–1 item; 2201.1. According to General Records Schedule (GRS) 5.1 item 010, DAA–GRS–2017– 0003–0001, temporary destroy transitory records, messages coordinating schedules, appointments, and events when no longer needed for business use, or according to agency predetermined time or business rule.

6000.1. Health Records Folder File or CHR (Consolidated Health Record).
This records series contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system.

a. Health Records Folder. This file constitutes the active medical or clinical records segment of the CHR. It completely documents diagnostic examinations and definitive medical, surgical, psychiatric, and dental care or treatment rendered a patient at a VA health care facility or at VA expense. It contains, in written and graphic form, the diagnostic; treatment and sociological information compiled by various members of the medical care team who participated in the care of a patient during one or more courses of treatment. In addition, it is intended to meet the legal, administrative, teaching and research needs of the VA medical staff, and provides a means of studying and evaluating the type of care rendered. VA and other monetary benefits are sometimes decided by use of information from the Health Records Folder.

   Temporary; retain in VA health care facility until 3 years after last episode of care, and then convert to an inactive medical record. (N1-15-91-6, Item 1a)

b. Outpatient Treatment Folders currently on hand at VA medical facilities.

   Temporary; transfer to Health Record File or CHR and retain in VA health care facility until 3 years after last episode of care, then convert to a Perpetual Medical Record and an Inactive Medical Record. (NI-15-87-4, Item 4a)

The information retained by the CCRA system is listed in Section 3.1. (This information pertains only to records that are maintained in the CCRA system.) Feeder records are original records and are maintained in accordance with VistA, Cerner, AWS GovCloud and MPI records retention policy and the VistA, Cerner, and MPI PIA documents.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

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

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

HSRM does not use real data for development, research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:
Privacy Risk: Increased risk of exposure of records are retained longer than the designated retention period.

Mitigation: CCRA follows VHA RCS 10-1 and all records are retained based on what is outlined in VHA RCS 10-1. When it is time for dissemination, CCRA follows the steps listed 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***
Cerner	Receive Community Care Consults	Name, Gender, DOB, Phone Number(s), Email, Preferred Contact Method, Residential and Mailing Addresses, Preferred Language, Translator Required, SSN, ICN, EDIPI, DFN Number(s), Race, Ethnicity, Religion, Provisional Diagnosis, Category of Care, Services Requested	Transmitted via HL7 messages from Cerner
Community Care Reimbursement System (CCRS)	Send referral information so that Community Care Third Party Payors can be Reimbursed	Veteran Demographics, Referral Details, Services Requested, Program Authority, Insurance Details, Community Provider Information, Appointment Information	Transmitted via secure file transport protocol (SFTP) within the VA network, files at rest are encrypted, HSRM consumes the information CCRS provides

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*
Corporate Data Warehouse (CDW)	Referral data to be housed in the corporate data warehouse	Veteran Demographics, Referral Details, Services Requested, Program Authority, Insurance Details, Community Provider Information, Appointment Information	Transmitted to CDW from the various Structured Query Language (SQL) databases using Hypertext Transfer Protocol Secure (HTTPS)
Data Access Service (DAS)	Referrals are transmitted through DAS to be sent to third-party administrators (TPA)	Veteran Demographics, Referral Details, Services Requested, Program Authority, Insurance Details, Community Provider Information, Appointment Information	Transmitted via a representational state transfer web service over HTTPS, DAS consumes the information HSRM provides
Electronic Claims Adjudication Management System (eCAMS)	Process out of network claims	Veteran Demographics, Referral Details, Services Requested, Program Authority, Insurance Details, Community Provider Information, Appointment Information	Transmitted via SFTP HTTPS, HSRM provides the information eCAMS consumes
ECR	Notify VA of Emergency Care	Veteran Demographics, Provider Details, Chief Complaint, Diagnosis	Transmitted via a SOAP web service over HTTPS; ES provides the information HSRM consumes
ES	Evaluate eligibility for care in the community	Veteran eligibility information	Transmitted via a SOAP web service over HTTPS; ES provides the information HSRM consumes
IAM SSOe	Provides VA users access to HSRM and ECR	Authentication information as provided by SSOe	Transmitted via Security Assertion Markup Language (SAML) assertion passed as part of the redirect to our

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*
			page; HSRM consumes the information SSOe provides
IAM SSOi	Provides Community Providers access to HSRM	Authentication information as provided by SSOi	Transmitted via SAML assertion passed as part of the redirect to our page; HSRM consumes the information SSOi provides
MPI	Update Veteran demographics	Name, Gender, Phone Number(s), Residential and Mailing Addresses, SSN	Transmitted via a SOAP web service over HTTPS
Program Integrity Tool (PIT)	Evaluate waste, fraud and abuse	Veteran Demographics, Referral Details, Services Requested, Program Authority, Insurance Details, Community Provider Information, Appointment Information	Transmitted via SFTP HTTPS, HSRM provides the information PIT consumes
PPMS	Retrieve Community Provider information that may be associated to a referral	Provider Demographics	Transmitted via a representational state transfer web service over HTTPS, HSRM consumes the information PPMS provides
SEOC / One Consult	Retrieve VA Standard Episodes of Care that may be associated to a referral	SEOC data, with associated treatment codes (this is not associated to Veterans or referrals at transmit time)	Retrieved from SharePoint site via a representational state transfer web service over HTTPS
Veterans Data Integration and Federation (VDIF)	Provide VA and Community Providers access to view Veteran clinical data	Medical Conditions, Allergies, Medications, Documents, Immunizations, Vital Signs, Lab Results, Diagnostic Studies,	Transmitted via SOAP web services over HTTPS

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*
		Procedures, Histories, Encounters, Appointments, Care Team, Cohorts, Demographics	
VistA	Receive Community Care Consults	Name, Gender, DOB, Phone Number(s), Email, Preferred Contact Method, Residential and Mailing Addresses, Preferred Language, Translator Required, SSN, ICN, EDIPI, DFN Number(s), Race, Ethnicity, Religion, Provisional Diagnosis, Category of Care, Services Requested	Transmitted via HL7 messages from HSRM which VistA consumes

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:
Privacy Risk: PII may be accidently released to unauthorized individuals.

Mitigation: Information is only accessible to authorized individuals who gain access with their personal identity verification (PIV) card and providing a pin. All users must take HIPAA and VA Privacy and Security training. Cognosante follows National Institute of Standards and Technology (NIST) audit accountability standards, and VA 6500, with audit logs monitored periodically.

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

CCRA SaaS and Integration Development shares referral information with the external care providers specific to the referral via HSRM.

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***
HSRM Commercial Off the Shelf (COTS)	Information related to the referral, scheduling, and status is needed by the provider	Name, SSN, DOB, Mailing Address, Zip Code, Phone Number(s), Emergency Contact, Information Health Insurance (Beneficiary Numbers, Account Numbers), Current Medications, Previous Medical Records,	SORN: HSRM – VA (180VA10D) 38 U.S.C. 8111 and 10 U.S.C. 1104 for Military Treatment Facilities,	Data is shared with external providers via HTTPS

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*
		Race/Ethnicity, EDIPI, Gender Beneficiary Type (whether the individual is a Veteran or spouse of a Veteran), Contact Notes (additional information regarding contacting the patient), Preauthorization, Preferred Contact Method, Preferred Language, Translator Required, Veterans Choice Eligibility, Service-Connected Disability	Indian Health Services 25 U.S.C. Sections 1645,1647; 38 U.S.C. Sections 523(a), 6301-6307, 8153; Academic sharing agreements 38 U.S.C. 8153; Legal authorities covering the CCRA use of PHI and PII for medical care are Public Law 115-26, Public Law 104-191, and 45 C.F.R. 164.506; SORN routine use under the authority of Title 44 U.S.C.	
AWS GovCloud	AWS hosts HSRM	AWS hosts the HSRM system. No data is shared	Authority to Operate (ATO) and an Interconnection Security Agreement (ISA) and Memorandum	Transmitted via Trusted Internet Connection (TIC)-Virtual Private Network (VPN)

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*
			of Understanding (MOU)	
Optum	To provide referrals to CCRA, initiating the process	Veteran demographics, Referral Details, Services Requested, Program Authority, Insurance Details, Community Provider Information, Appointment Information	Contract, ISA/MOU, and Interface Control Document (ICD)	Transmitted via a representational state transfer web service over HTTPS, Optum consumes the information HSRM provides
TriWest	To provide referrals to CCRA, initiating the process	Veteran demographics, Referral Details, Services Requested, Program Authority, Insurance Details, Community Provider Information, Appointment Information	Contract, ISA/MOU, and ICD	Transmitted via a representational state transfer web service over HTTPS, TriWest consumes the information HSRM provides

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:
Privacy Risk: PII may be accidently released to unauthorized individuals.

Mitigation: Information is only accessible to authorized individuals who gain access with their approved SSOe-provided credentials and provide a password. All users must take HIPAA and VA privacy and security training. Audit logs are in place. For external users, ID.me is used for authentication and VA SSOe is used for authorization.

Section 6. Notice

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.
This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

HSRM imports data from VistA, Cerner, AWS GovCloud, and MPI; no new PHI/PII is collected from individuals. Notice is provided to individuals when data is collected for VistA or Cerner. Privacy notices are provided at the point of service at the medical center where the Veteran receive care, in accordance with VHA Handbook 1605.4, Notice of Privacy Practices.
Notice of privacy practices are available on the https://www.va.gov/privacy/

Each of the above notices includes information on how to report any use of information that is not in accordance with the collection. Reference Error! Reference source not found. for a link to the notice of privacy practices provided at all VAMCs.

System of records notices that apply to the collection, use and disclosure of information within this data collection. Link: https://www.oprm.va.gov/privacy/systems_of_records.aspx

- 23VA10NB3, Non-VA Care (Fee) Records – VA (July 30, 2015)
- 24VA10A7, Patient Medical Records – VA (October 12, 2020)
- 79VA10P, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (December 23, 2020)
- 97VA10, Consolidated Data Information System – VA (December 23, 2020)
- 121VA1007, National Patient Databases – VA (February 12, 2018)
- 147VA10, Enrollment and Eligibility Records – VA (August 17, 2021)
- 180VA10D, HealthShare Referral Manager (HSRM) – VA (August 17, 2021)

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

HSRM imports data from VistA, Cerner, AWS GovCloud, and MPI; no new PHI/PII is collected from individuals. Notice is provided to individuals when data is collected for VistA or Cerner. YOUR PRIVACY RIGHTS 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, we are not required to agree to such restriction, except in the case of a disclosure restricted under 45 C.F.R. § 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 in full. However, VHA is not legally able to accept an out-of-pocket payment from a Veteran for the full cost of a health care service or visit. We are only able to accept payment from a Veteran for co-payments. Therefore, this provision does not apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of your health information to a health plan for the purpose of receiving payment for health care services 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 no longer make the restriction request valid or you revoke it.

Reference Error! Reference source not found. for the complete notice.

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

HSRM imports data from VistA, Cerner, AWS GovCloud, and MPI; no new PHI/PII is collected from individuals. Notice is provided to individuals when data is collected for VistA or Cerner. Individuals have a right to contact the VHA call center to gain access to their information.

Reference Error! Reference source not found. for a link to the notice of privacy practices provided at all VAMCs, which includes the following:

Other Uses and Disclosures with Your Authorization. We may use or disclose your health information for any purpose based on 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 written authorization or permission to use or disclose your health information, you may revoke that permission, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your health information except to the extent that VHA has relied on your written authorization. Please understand that we are unable to take back any uses or disclosures we have already made based on your authorization.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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: If notice is not provided in a timely manner, an individual might give information that they do not want to be shared.

Mitigation: CCRA collects no information from Veterans. Information in this system is gathered through other VA systems. Veteran and Beneficiaries are provided notice of Privacy Practices in and through several different locations before their information is collected.

Reference Error! Reference source not found. for the complete notice and the CHAMPVA Guide.

Section 7. Access, Redress, and Correction

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

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

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

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

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

Reference Error! Reference source not found. for a link to the notice of privacy practices provided at all VAMCs, which includes the following:

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

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

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

Individuals have a right to contact the VHA call center at 855-673-4357 to gain access to their information.

Reference Error! Reference source not found. for a link to the notice of privacy practices provided at all VAMCs, which includes the following:

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

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

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

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

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

Individuals have a right to contact the VHA call center at 855-673-4357 to gain access to their information.

Reference Error! Reference source not found. for a link to the notice of privacy practices provided at all VAMCs, which includes the following:

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

policy, from you to receive communications containing your health information:

- At a mailing address (e.g., confidential communications address) other than your permanent address
- In person, under certain circumstances

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Individuals have a right to contact the VHA call center at 855-673-4357 to gain access to their information.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

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

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

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

Follow the format below:

Privacy Risk: There is a risk information provided to CCRA is incorrect resulting in false appointment information being displayed.

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

Section 8. Technical Access and Security

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

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

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

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

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

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

There are two distinct access-provisioning mechanisms—one for internal VA employees and contractors and one for external health care providers. Both are described in this section.

VA Internal Authentication, SSOi

The IAM SSOi service is an authentication service specifically designed for controlling access for VA internal users (employees and contractors) accessing VA applications. This service enhances the user experience by reducing the time associated with multiple logon and logoff activities that require application-specific identifiers and passwords. The service also enables enriched password management and reduction in help desk support.

CCRA is integrated with the VA IAM SSOi for all internal user-facing VA applications, which provides two-factor authentication compliance. The VA PIV card provides the required second piece to the two-factor authentication. To achieve this authentication there is an SSOi SAML partnership in which the SSOi service is the identity provider, and the application (typically external to VA) is in the service provider role. SSOi uses a previously authenticated session user as the subject for this identity provider and generates a signed and encrypted new SAML token for the partner application to process.

Support for government-approved algorithms must be provided (e.g., signature: rsa-sha256 and encryption: AES256).

External Authentication, SSOe

The IAM SSOe service is an authentication service specifically designed for controlling access for external users accessing VA applications. (For CCRA this will be community health providers and their administrators.) This service enhances the user experience by reducing the time associated with multiple logon and logoff activities that require application-specific identifiers and passwords. The service also enables enriched password management and reduction in help desk support.

The SSOe service authenticates users with Cloud Service Provider (CSP) credentials and other externally issued credentials. SSOe retrieves user information from VA authoritative sources to augment the user data provided to integrated applications, and this additional data provides the VA identity context of the user.

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 subcontractors are subject to confidentiality and nondisclosure agreements from Cognosante and VA. The CCRA system is operated and maintained entirely by Cognosante and hosted in the AWS GovCloud environment. System access requires a VA-issued PIV and government-furnished equipment. All contractors require Talent Management System (TMS) training, annual Privacy and HIPAA-Focused Training (10203), and annual VA Privacy and Information Security Awareness and Rules of Behavior (10176).

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.

HSRM is hosted in the AWS GovCloud. VA employees, contractors, and subcontractors are required to complete VA privacy training annually within TMS, including Privacy and HIPAA-Focused Training (10203) and VA Privacy and Information Security Awareness and Rules of Behavior (10176).

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

If Yes, provide:

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

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

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

CCRA SaaS and Integration Development was granted a full 3-year authority to operate (ATO) on June 16, 2022, which expires June 15, 2025. The FIPS system classification is high.

Section 9 – Technology Usage

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

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

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

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

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

Yes, FedRAMP hosted within VAEC

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

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

Not applicable, FedRAMP hosted within VAEC

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, FedRAMP hosted within VAEC

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, FedRAMP hosted within VAEC

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, FedRAMP hosted within VAEC

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AC	**Access Control**
AC-1	Access Control Policy and Procedures
AC-2	Account Management
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-5	Separation of Duties
AC-6	Least Privilege
AC-16	Security Attributes
AC-21	Information Sharing
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress

ID	Privacy Controls
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 provided in this Privacy Impact Assessment is true and accurate.

Michael D Hartmann 1612370

Digitally signed by Michael D Hartmann 1612370
Date: 2022.07.05 11:05:25 -06'00'

Privacy Officer, Michael Hartmann

KIMBERLY KEENE

Digitally signed by KIMBERLY KEENE
Date: 2022.07.05 15:27:27 -04'00'

Information Systems Security Officer, Kimberly Keene

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2022.07.07 13:25:39 -05'00'

Information Systems Owner, Chris Brown

APPENDIX A

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

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

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

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

YOUR PRIVACY RIGHTS

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

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

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

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

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

- At a mailing address (e.g., confidential communications address) other than your permanent address.
- In person, under certain circumstances.

Right to Request Restriction. You may request that we not use or disclose all or part of your health information to carry out treatment, payment or health care operations, or that we not use or disclose all or part of your health information with individuals such as your relatives or friends involved in your care, including use or disclosure for a particular purpose or to a particular person.

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

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

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

Right to Receive an Accounting of Disclosures. You have the right to know and request a copy of what disclosures of your health information have been made to you and to other

individuals outside of VHA. To exercise this right, you must submit a written request to the facility Privacy Officer at the VHA health care facility that provides your care.

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

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

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

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

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

Treatment. We may use and disclose your health information without your authorization for treatment or to provide health care services. This includes using and disclosing your information for:

- Emergency and routine health care or services, limited to labs and x-rays, clinic visits, inpatient admissions
- Contacting you to provide appointment reminders about treatment alternatives
- Seeking placement in community living centers or skilled nursing homes
- Providing or obtaining home-based services or hospice services
- Filling and submitting prescriptions but not for medications, supplies, and equipment
- Coordination of care, including care from non-VHA providers
- Communicating with non-VHA providers regarding your care through health information exchanges
- Coordination of care with DoD, including electronic information exchange

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

Examples:

1) A Veteran sees a VHA doctor who prescribes medication based on the Veteran's health information. The VHA pharmacy uses this information to fill the prescription.
2) A Veteran is taken to a community hospital emergency room. Upon request from the emergency room, VHA discloses health information to the non-VHA hospital staff that needs the information to

treat this Veteran.

3) A National Guard member seeks mental health care from VHA. VHA discloses this information to DoD by entering the information into a database that may be accessed by DoD providers at some future date.
4) A Veteran is seen by his community health care provider, who wants to review the Veteran's last blood work results from his VHA Primary Care visit for comparison. The community health care provider uses a local health information exchange to request and receive the results from VHA to better care for the Veteran.

Payment. We may use and disclose your health information without your authorization for payment purposes or to receive reimbursement for care provided. This includes using and disclosing your information for:

- Determining eligibility for health care services
- Paying for non-VHA care and services, including but not limited to, CHAMPVA, Choice and fee basis
- Coordinating benefits with other insurance payers
- Finding or verifying coverage under a health insurance plan or policy
- Pre-certifying insurance benefits
- Billing and collecting for health care services provided by VHA
- Reporting to consumer reporting agencies regarding delinquent debt owed to VHA.

Examples:

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

Health Care Operations. We may use or disclose your health information without your authorization to support the activities related to health care. This includes using and disclosing your information for:

- Improving quality of care or services
- Conducting Veteran and beneficiary satisfaction surveys
- Reviewing competence or qualifications of health care professionals
- Providing information about treatment alternatives or other health-related benefits and services
- Performing process reviews and root cause analyses
- Conducting health care training programs
- Managing, budgeting and planning activities and reports
- Improving health care processes, reducing health care costs and assessing organizational performance
- Developing, maintaining and supporting computer systems
- Addressing patient complaints
- Legal services
- Conducting accreditation activities
- Certifying, licensing, or credentialing of health care professionals
- Conducting audits and compliance programs, including fraud, waste and abuse investigations

Examples:

1) Medical Service, within a VHA health care facility, uses the health information of diabetic Veterans as part of a quality-of-care review process to determine if the care was provided in accordance with the established clinical practices.
2) A VHA health care facility discloses a Veteran's health information to the Department of Justice (DOJ)

attorneys assigned to VA for defense of VHA in litigation.

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

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

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

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

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

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

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

Law Enforcement. We may disclose your health information without your authorization to law enforcement agencies for law enforcement purposes when applicable legal requirements are met. This includes disclosing your information for:

- Identifying or apprehending an individual who has admitted to participating in a violent crime
- Reporting a death where there is a suspicion that death has occurred as a result of a crime
- Reporting Fugitive Felons
- Investigating a specific criminal act
- Routine reporting to law enforcement agencies, such as gunshot wounds
- Providing certain information to identify or locate a suspect, fugitive, material witness, or missing person

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

government benefit programs, other government regulatory programs, and agencies that enforce civil rights laws.

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

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

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

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

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

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

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

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

- A researcher is preparing a plan for a research project. For example, a researcher needs to examine patient medical records to identify patients with specific medical needs. The researcher must agree to use this information only to prepare a plan for a research study; the researcher may not use it to contact you or actually conduct the study. The researcher

also must agree not to remove that information from the VHA health care facility. These activities are considered preparatory to research.
- The IRB approves a waiver of authorization to use or disclose health information for the researchbecause privacy and confidentiality risks are minimal and other regulatory criteria are satisfied.
- A Limited Data Set containing only indirectly identifiable health information (such as dates, unique characteristics, unique numbers or zip codes) is used or disclosed, with a data use agreement (DUA) in place.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

When We Will Not Use or Disclose Your Health Information

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

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

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

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