Privacy Impact Assessment for the VA IT System called:

Clinical Decision Support Platform (CDSP) Veterans’ Health Administration (VHA) Enterprise Program Management Office (EPMO)

eMASS ID #1411

Date PIA submitted for review:

3/26/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Nancy Katz-Johnson*	*nancy.katzjohnson@va.gov*	*(203) 535-7280*
Information System Security Officer	*Jennifer Huba*	jennifer.huba@va.gov	(412) 295-4917
Information System Owner	*Shane Elliott*	*shane.elliott@va.gov*	*(909) 503-2889*

Abstract

The abstract provides the simplest explanation for "what does the system do for VA?".

Clinical Decision Support Platform (CDSP) is the core system to enable externalized clinical decision support tools and services for both Vista/CPRS as well as Oracle Health. CDSP is a standards-based platform that leverages Substitutable Medical Applications and Reusable Technologies (SMART) on Fast Healthcare Interoperability Resources (FHIR) technology to deliver digital tools that can be accessed from within the electronic health record and provide guideline-based recommendations on care for patients. This system consists of technical infrastructure to launch from within the electronic health record while maintaining patient context, interact with electronic health record data, authenticate clinicians, maintain appropriate security, and other capabilities. CDSP serves as a comprehensive clinical decision support platform that can scale to provide additional services to meet changing clinical needs.

Overview

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

1 General Description

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

Supported Business Functions: Provide Clinical Decision Support - Provide Clinical Decision Support augments clinical decision-making by providing health care professionals with knowledge-enriched, disease-specific recommendations for treatments, tests and referrals based on individual patient profiles. It also includes the ability to identify potential problems or trends within the patient community. This function leverages coded clinical data, global medical knowledge and institutional protocols.

Supported VHA Capabilities: Clinical Decisions Support (incl. reminders) - Clinical decision support (CDS) provides clinicians, staff, patients or other individuals with knowledge and person-specific information, intelligently filtered or presented at appropriate times, to enhance health and health care. CDS encompasses a variety of tools to enhance decision-making in the clinical workflow. CDS tools include computerized alerts and reminders to care providers and patients; clinical guidelines; condition-specific order sets; focused patient data reports and summaries; documentation templates; diagnostic support; and contextually relevant reference information, among other tools. CDS supports stakeholders across venues, drives panel and population management, and facilitates healthcare processes, for example via closed-loop task management.

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

VA Owned and VA Operated - Veterans Health Administration (VHA-10)

2. Information Collection and Sharing

C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

System is deployed VA-wide. Clinicians access data for patients via VA managed clinical endpoints after authenticating with clinical credentials. The system has the capability to retrieve data on all patients whose information is stored in VistA, CDW, and other connections detailed in the associated charts. Clinical data may be stored for the purposes of patient care in secured cloud databases hosted within VAEC. Data use and limitations are detailed in the corresponding tables."

Check if Applicable	**Demographic of individuals**
☒	Veterans or Dependents
☒	VA Employees
☒	Clinical Trainees
☒	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

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

Clinical Decision Support Platform (CDSP) is a privacy sensitive system that accesses and processes Personally Identifiable Information on Veterans, VA employees and contractors, clinical trainees.

E. *What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*

Clinical Decision Support Platform (CDSP) is the core system to power clinical decision support applications. It enables rapid development and deployment of applications that follow Substitutable Medical Applications and Reusable Technologies (SMART) family of standards such as SMART on FHIR (Fast Healthcare Interoperability Resources) and CDS Hooks. CDSP facilitates the launch of CDS applications from within the VA Electronic Health Record (EHR) – CPRS and CCOW vault patient context synchronization. The system encompasses technical infrastructure and shared capabilities to interact with electronic health record data, as well as specific components providing clinical decision support such as Covid19 Patient Manager (CPM), Lung Cancer Screening Platform (LCSPv2), and Precision Oncology (PO).

F. Are the modules/subsystems only applicable if information is shared?

Yes.

G. Is the system operated in more than one site to include primary and secondary 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?

CDSP is a PaaS. This system will be used in multiple VA Medical Centers and is hosted within the VAEC. The same controls will be used across all sites in accordance with VAEC VA Enterprise Cloud Policy and requirements. This application is a standards-based (utilizing Substitutable Medical Application and Reusable Technologies (SMART) on Fast Healthcare Interoperability Resources (FHIR) web application, and it is through use of these standards that consistency of the PII accessed by the system will be maintained.

3. Legal Authority and System of Record Notices (SORN)

H. What is the citation of the legal authority?

The legal authority to operate this application is: SOR 24VA10A7 Patient Medical Records; Title 38, USC 501(b) and 304.

I. What is the SORN?

SOR 24VA10A7 – Patient Medical Records. https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

No. The current SORN covers cloud usage and storage and does not need to be updated at this time the application operates in accordance with SOR 24VA10A7.

4. System Changes

K. Will the business processes change due to the information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

I. Will the technology changes impact information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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 Information collected, used, disseminated, created, or maintained in the system.

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name
☒ **Full** Social Security Number
☒ **Partial** Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☐ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a Different Individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account Numbers
☐ Certificate/License

Numbers[1]

☐ Vehicle License Plate Number

☐ Internet Protocol (IP) Address Numbers

☒ Medications

☒ Medical Records

☒ Race/Ethnicity

☐ Tax Identification Number

☐ Medical Record Number

☒ Sex

☒ Integrated Control Number (ICN)

☒ Military History/Service Connection

☐ Next of Kin

☐ Date of Death

☐ Business Email Address

☐ Electronic Data Interchange Personal Identifier (EDIPI)

☒ Other Data Elements (List Below)

Other PII/PHI data elements:

- Patient Age
- Veteran Health Identity Card Identifier
- Patient photograph (Veteran Health Identity Card)
- Preferred name
- Marital status
- Problem list
- Diagnoses
- Vital signs
- Diagnostic tests
- Laboratory results
- Procedure history
- Genetic data
- Progress notes
- Care Assessment Need (CAN) Scores
- Appointment information
- Clinical care reminders
- From VA employees:
    - Provider/Clinician Names
    - VistA Designated User Identifier (DUZ)
    - Identity and Access Management (IAM) SecID
    - Provider Internal Entry Number (IEN)
    - Provider contact information; email Addresses
- From VA Contractors:
    - Employee Names
    - VistA Designated User Identifier (DUZ)
    - Identity and Access Management (IAM) SecID
    - Employee contact information, Email Addresses
- Clinical Trainees
    - Names

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

- VistA Designated User Identifier (DUZ)
- Identity and Access Management (IAM) SecID
- Trainee Email Addresses

1.2 List the sources of the information in the system

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

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The information is accessed from the electronic health record stored in VistA. Some of this information has been provided by the individual in the past while other information is gathered from the individual's medical history within the VA. The system uses this information to help clinicians identify a patient and provide them with medication information to aid with treatment plans and patient visits.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

CDSP accesses and aggregates information to allow the clinician to make decisions based on all information available to the Platform. This information is gathered from a variety of sources that may include the individual and VA datastores.

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

CDSP is a collection of tools that processes/analysis medical information to provide recommendations for potential action to clinicians. Information that providers enter into CDSP is stored in our Database (e.g., LCSPv2). Recommendations for care provided by features are not stored within CDSP, and the decision/determination of the clinician is recorded on other systems such as VISTA. Care recommendations that are part of patients' chart are stored in the appropriate EHR.

1.3 Methods of information collection

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

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

The information is accessed from the electronic health record stored in VistA via Clinical Health API over HTTPS.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

CDSP does not collect information in a form and is not subject to the Paperwork Reduction Act. The OMB control number and agency form number is not applicable in this situation.

1.4 Information checks for accuracy, and how often will it be checked.

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

CDSP accesses and processes information from other VA sources. The source systems have controls in place to check for accuracy and these controls are "Inherited" for CDSP.

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

System does not utilize a commercial aggregator.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

24VA10A7/ 85 FR 62406 Patient Medical Records-VA 2020-21426.pdf (https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf) Authority: Title 38, United States Code, Sections 501(b) and 304.

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: *The collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

Principle of Minimization: *The information is directly relevant and necessary to accomplish the specific purposes of the program.*

Principle of Individual Participation: *The program, to the extent possible and practical, collects information directly from the individual.*

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

Follow the format below when entering your risk assessment:

Privacy Risk: The system accesses and displays PII and other sensitive PHI. If this information was breached or accidentally released to inappropriate parties or the public, it could result in personal, and/or emotional harm to the individuals whose information were inappropriately accessed.

Mitigation: The system is careful to display only the information necessary to accomplish the VA mission of assisting physicians with making clinical decisions about caring for individual patients. The clinician-facing application requires authentication and authorization to ensure that the user accessing the application is appropriately authorized to access the data displayed by the application. Workstations at VA Medical Centers are designed to maximize physical security of the information being displayed on a given screen. The system logs are securely maintained, and access to the audit logs is limited to personnel with security - related roles and auditors.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Patient Name	Patient's full name including first name, middle initial, and last name. Used to identify patient.	Not used
Patient Social Security Number (SSN)	Used as a patient identifier, last 4 is only used.	Not used

Patient Date of Birth (DOB)	Used to identify patient age and confirm patient identity.	Not used
Patient Age	Used to identify patient age and confirm patient identity.	Not used
Patient Sex	Used to identify patient and confirm patient identity.	Not used
Patient Preferred Name	Used to identify patient and confirm patient identity.	Not used
Patient Race	Used to identify patient and confirm patient identity.	Not used
Patient Ethnicity	Used to identify patient and confirm patient identity.	Not used
Patient Marital Status	Used to identify patient and confirm patient identity.	Not used
Patient Phone Number(s)	Used to reach out to the patient to provide updates on care.	Not used
Patient Photograph (Veteran Health Identity Card)	Used to identify patient and confirm patient identity.	Not used
Patient Care Assessment Need (CAN) Scores	Used to assist clinical staff in recommending care.	Not used
Patient Medications List	Patient’s current medication listing. Used to assist clinical staff in recommending care.	Not used
Patient Medical Records	Patient’s medical history. Used to assist clinical staff in recommending care.	Not used
Patient Service Connection	Patient’s service connection related to any conditions. Used to assist clinical staff in determining coverage.	Not used
Patient Integrated Control Number (ICN)	Internal record tracking number for each Patient, SSN reduction initiative.	Not used
Patient Problem List	List of patient’s issues for each Patient. Used to assist clinical staff in recommending care.	Not used
Patient Diagnoses	List of Patient’s Diagnoses. Used to assist clinical staff in recommending care.	Not used
Patient Vital Signs	History of Patient’s vital signs. Used to assist clinical staff in recommending care.	Not used
Patient Diagnostic Tests	History of Patient’s Diagnostic Tests. Used to assist clinical staff in recommending care.	Not used

Patient Laboratory Results	History of Patient’s Lab Results. Used to assist clinical staff in recommending care.	Not used
Patient Genetic Data	Used to assist clinical staff in recommending care.	Not used
Patient Progress Notes	Used to assist clinical staff in recommending care.	Not used
Appointment Information	Used to assist clinical staff in recommending care.	Not used
Clinical care reminders	Reminders supplied to clinicians, used to assist clinical staff in recommending care.	Not used
VistA Designated User Identifier (DUZ)	The users’ VistA identifier. Used to identify user and match records.	Not used
Identity and Access Management (IAM)	SSOi identity for authentication. Used to authenticate clinician.	Not used
SecID	Unique individual Security ID number per user. Used to identify user.	Not used

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

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

The system accesses and processes information for Veteran patients. This data is used to compute recommendations for next steps in care for patients. These recommendations and data are displayed to authenticated physicians so that they may make decisions about next steps in the prognosis and care of the patient.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

CDSP is a collection of tools that processes/analysis medical information to provide recommendations for potential action to clinicians. Care recommendations that are part of patients' chart are stored in the appropriate EHR. They are not stored in CDSP, the decision/determination of the clinician is recorded on other systems such as VistA.

2.3 How the information in the system is secured.

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

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

Information in Transit is encrypted via Hypertext Transfer Protocol Secure in Accordance With VA Enterprise Cloud requirements. Information at rest is encrypted using AWS native solutions: AWS Key Management Service (KMS) and AWS Aurora which have received FedRAMP High authorization.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

Information in Transit is encrypted via HTTPS IAW VAEC requirements. CDSP does not store full Social Security Numbers – only the last 4 digits. CDSP follows VAEC requirements for data at rest protection and encryption. SSNs are only available to authenticated users who are authorized to view those SSNs. Additionally, the API we call from has headers on the response that prevent caching of sensitive data.

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

Information in Transit is encrypted via HTTPS IAW VAEC requirements. CDSP protects data at rest in accordance with VAEC requirements. CDSP utilizes AWS native solutions: AWS Key Management Service (KMS) and AWS Aurora which have received FedRAMP High authorization. The controls in place to assure that the information is handled in accordance with the uses described above include mandatory online information security and Privacy and HIPAA training.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

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

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

2.4a How is access to the PII determined?

The system utilizes SSOi for authorization of users. Access to the system is restricted to authorized VA Medical Center personnel.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Yes – documented in the CDSP Access Control Standard Operating Procedures in which all users have access to this document.

2.4c Does access require manager approval?

Yes – documented in the CDSP Access Control Standard Operating Procedures in which all users have access to this document.

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

Yes - documented in the CDSP Access Control Standard Operating Procedures in which all users have access to this document.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

The system utilizes SSOi for authorization of users. Access to the system is restricted to authorized VA Medical Center personnel who have access to the underlying data. Controls are inherited from VAEC, as well as responsibilities of the ISO and ISSO. DAR is encrypted using best practices within the VAEC. In addition, project managers and approving bodies are responsible for vetting personnel who have access to PII/PHI. Personnel who have access to PII/PHI on this system are required to undergo training and are beholden to VA policies and procedures.

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

CDSP currently retains the following information:

- Patient Name
- Last 4 SSN
- Date of Birth
- Age
- Patient Sex
- Patient Personal Phone Number(s)
- Patient ICN
- Provider SecID
- Provider IEN
- Provider Name(s)
- Provider Email Addresses
- Clinical Care Reminders.
- Problem list
- Diagnoses
- Vital signs
- Diagnostic tests
- Laboratory results
- CT scans
- Tobacco use history

The system that feeds into the system is covered by SORN 24VA10A7 and follow the retention requirements: In accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6.

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

The system that feeds into the system is covered by SORN 24VA10A7 and follow the retention requirements in accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1) (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf), Chapter 6

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. Please work with the system VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

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

The system that feeds into the system is covered by SORN 24VA10A7 and follows the retention requirements Records Control Schedule 10-1 (va.gov) (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf).

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

Records Control Schedule 10-1 (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf). "POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: In accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3). PHYSICAL, PROCEDURAL, AND ADMINISTRATION. rcs10-1.pdf (va.gov)"

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

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

"Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle Bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.
https://www.va.gov/vapubs/search_action.cfm?dType=1 ."

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training, and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

CDSP does not use PII for research, testing, or training.

<u>3.6 PRIVACY IMPACT ASSESSMENT: Retention of information</u>

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document in this section).

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

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

<u>Principle of Minimization:</u> The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

<u>Principle of Data Quality and Integrity:</u> The PIA should describe 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:

<u>Privacy Risk:</u> There is a risk that the information maintained by CDSP could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

<u>Mitigation:</u> To mitigate the risk posed by excessive information retention; CDSP adheres to the VA RCS schedules for each category of data it maintains. When the retention limit is reached for a record, the data will be disposed of by the appropriate identified party (given that this system is cloud-based and hosted within VAEC) via the method determined most fitting of the particular data type as described in question 3.4. CDSP ensures to the extent that is possible that all personnel involved with the collection, use and retention of data are trained in the correct process for collecting, using, and retaining data. All other data retention and disposal matters fall under the scope of VAEC.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a CDSP consists of 2 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CDSP and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Amazon Web Service (AWS) Aurora Housed in the Clinical Decision Support (CDS) VAEC AWS	**Yes**	**Yes**	• Patient Name • Last 4 SSN • Date of Birth • Patient Sex • Patient Personal Phone Number(s) • Patient ICN • Provider SecID • Provider IEN • Provider Name(s)	This data is received from other systems and stored for performance reasons.	Encryption at rest, encryption in transit. Usage of AWS Managed Services with FedRAMP high authorization.

			• Provider Email Addresses • Clinical Care Reminders		
Lung Cancer Screening Database (LCS DB)	Yes	Yes	• Patient name • SSN (Last 4) • Patient Age • Problem list • Diagnoses • Vital signs • Diagnostic tests • Laboratory results • CT scans • Tobacco use history	Utilized to assist in clinical care recommendations.	Encryption at rest, encryption in transit. Usage of AWS Managed Services with FedRAMP high authorization.

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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***
VHA Lighthouse Clinical Health API	Veteran health data.	• Patient name • Patient date of birth • Patient Internal Control Number (ICN) • Last four digits of patient SSN • Patient sex • Patient sex at birth • Patient race • Patient ethnicity • Patient marital status • Patient problem list • Patient Medical Records • Patient Military History/Service • Patient diagnoses • Patient vital signs • Patient diagnostic tests • Patient laboratory results	Lighthouse clinical FHIR APIs (REST 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***
		• Patient medications • Patient procedure history • Patient progress notes • Patient contact information	
VistA Imaging	Support of Precision Oncology and cancer treatment.	• Patient name • Patient date of birth • Patient laboratory results • Patient genetic risk markers	We send this information to VistA Imaging via APIs (XML over HTTPS)
Data Access Services	Support of Precision Oncology and cancer treatment.	• Patient name • Patient date of birth • Patient laboratory results • Patient genetic risk markers	We retrieve this information from DAS via S3 sync
Corporate Data Warehouse	Information necessary for Clinical Decision Support application to perform their function / calculations.	• Patient name • Patient date of birth • Patient Internal Control Number (ICN) • Patient problem list • Patient diagnoses	CDSP applications connect to CDW MSSQL

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Patient vital signs • Patient diagnostic tests • Patient laboratory results • Patient medications • Patient procedure history • Patient progress notes • Patient CAN scores	
VA Identity and Access Management Master Person Index (MPI) Veteran Health Identity Card Service (VHIC)	Correlation of various patients' and providers' identifiers. Display of patient photograph and basic demographic data to provider for quicker identification.	• Patient name • Patient date of birth • Patient Internal Control Number (ICN) • Last four digits of patient SSN • Patient sex • Patient sex at birth • Patient race • Patient ethnicity • Patient marital status • Patient personal phone number(s) • Patient email address	We retrieve data using MPI FHIR endpoint (REST over HTTPS) and VHIC SOAP API (XML 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***
		• Patient photograph (Veteran Health Identity Card) • Veteran Health Identity Card Identifier	
Office of Connected Care (OCC)	CDSP utilizes an OCC proxy service to check if a patient has a MyHealth*e*Vet Premium Account.	• Medical Records	CDSP uses a connection to make a call to the OCC Proxy API.
VistA	Veteran health data.	• Patient name • Patient date of birth • Patient Internal Control Number (ICN) • Last four digits of patient SSN • Patient sex • Patient sex at birth • Patient race • Patient ethnicity • Patient marital status • Patient problem list • Patient Medical Records • Patient Military History/Service	Electronically pulled via REST API's and Lighthouse clinical FHIR APIs (REST 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***
		• Patient diagnoses • Patient vital signs • Patient diagnostic tests • Patient laboratory results • Patient medications • Patient procedure history • Patient progress notes • Patient personal phone number(s) • Patient email address	
Imprivata Vergence (CCOW)	Veteran health data.	• Patient name • Patient ICN • VistA Identifiers • Provided Name • Provider Identifiers	Encrypted websocket connection to the CCOW agent (Vergence) running on the healthcare provider workstation.
Health Data Analytics Platform (HDAP) (Formerly known as Rockies)	Veteran health data.	• Patient name • SSN (Last 4) • Age • Problem list • Diagnoses • Vital signs • Diagnostic tests • Laboratory results • CT scans • Tobacco use history	There is a link to the application from CPRS, which opens in a browser tab. Access to the application will only occur from clinician-registered equipment with

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***
			access to CPRS or Cerner. Our continuous integration pipeline does not directly communicate with the virtual box where the application is deployed. Instead, the virtual box pulls the latest application version from the Docker registry. The credentials for the virtual box are stored in an Ansible vault file which is stored in a VA internal Github repository (“smart-on-fhir-infra”). It is encrypted using AES-256.

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

Discuss the privacy risks associated with the sharing of information within the VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).

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

Follow the format below:

<u>Privacy Risk:</u> The privacy risk associated with displaying data within the Department of Veterans Affairs is that the data may be disclosed to individuals who do not require access or have a need to know. Inappropriate/unauthorized disclosure heightens the threat of the information being misused.

Mitigation: The system is careful to display only the information necessary to accomplish the VA mission of assisting physicians with making clinical decisions about caring for individual patients. The clinician-facing application requires authentication and authorization to ensure that the user accessing the application is appropriately authorized to access the data displayed by the application.

Workstations at VA Medical Centers are designed to maximize physical security of the information being displayed on a given screen. The system logs are securely maintained, and access to the audit logs is limited to personnel with security - related roles and auditors.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

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

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

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

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

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

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

Data Shared with External Organizations

List IT System or External	*List the purpose of*	*List the specific PII/PHI data elements that are*	*List agreement*	*List the method of transmission and the*

Program Office information is shared/received with	***information being shared / received / transmitted***	***processed (shared/received/transmitted)***	***s such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***measures in place to secure data***
Cerner	To provide clinical decision support to the provider to better care for the patient.	• Patient name • Patient date of birth • Patient Internal Control Number (ICN) • Last four digits of patient SSN • Patient sex • Patient sex at birth • Patient race • Patient ethnicity • Patient marital status • Patient medical records • Patient problem list • Patient diagnoses • Patient vital signs • Patient diagnostic tests • Patient laboratory results • Patient medications • Patient procedure history • Patient progress notes • Patient appointment information	REST over HTTPS (FHIR API)	• Authority to Connect (ATC) • Memorandum of Understanding (MOU) Business Associate Agreement (BAA)

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: The privacy risk associated with displaying data within the Department of Veterans Affairs is that the data may be disclosed to individuals who do not require access or have a need to know. Inappropriate/unauthorized disclosure heightens the threat of the information being misused.

Mitigation: The system is careful to display only the information necessary to accomplish the VA mission of assisting physicians with making clinical decisions about caring for individual patients. The clinician-facing application requires authentication and authorization to ensure that the user accessing the application is appropriately authorized to access the data displayed by the application.

Workstations at VA Medical Centers are designed to maximize physical security of the information being displayed on a given screen. The system logs are securely maintained, and access to the audit logs is limited to personnel with security - related roles and auditors.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

In Accordance with 24VA10A7 which was published in the federal register 10/2/20 an explanation is provided for the authority, purpose, categories of information, routine uses and record access procedures (2020-21426.pdf [govinfo.gov]). All individuals who receive care at VHA are also provided with the Notice of Privacy Practices. Notice of Privacy Practice (NOPP): VHA Notice of Privacy Practices VHA Handbook 1605.04: Notice of Privacy Practices (VHA Notice of Privacy Practices & VHA Handbook 1605.04: Notice of Privacy Practices)

6.1b If notice was not provided, explain why.

All individuals who receive care at VHA are also provided with the Notice of Privacy Practices. Notice of Privacy Practice (NOPP): VHA Notice of Privacy Practices VHA Handbook 1605.04: Notice of Privacy Practices (VHA Notice of Privacy Practices [https://www.va.gov/files/2022-10/10-163p_%28004%29_-Notices_of_Privacy_Practices-_PRINT_ONLY.pdf] & VHA Handbook 1605.04: Notice of Privacy Practices [https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=11693])

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

Notice is provided to all Veterans who are eligible for care. The notice is also available at all VA medical centers as well as online:

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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

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

The Veterans' Health Administration (VHA) as well as the individual facilities request only information necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information to the VHA, this will prevent them from obtaining the benefits necessary to them. Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with the VA.

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

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

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

Information is used in accordance with the Privacy Act and is shared with VA employees when the information is needed in accordance with job requirements or when there is authority under b(1) of the Privacy Act. In addition, individuals may consent to additional uses of the information.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

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

Follow the format below:

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

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records. Additional mitigation is provided by making the

System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online.

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 The procedures that allow individuals to gain access to their information.

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

*7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. **For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

While this system does not create or maintain new patient information, directive 1605.01, Privacy and Release of Information, outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

While this system does not create or maintain new patient information, directive 1605.01, Privacy and Release of Information, outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

CDSP is governed by the Privacy Act.

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

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

The contact information for each medical center is listed in the System of Record Notice 24VA10A7. Individuals complete a written request for an amendment that is processed in accordance with VHA Directive 1605.01. Additionally, the Privacy Officers monitor that staff are aware of record access and amendment processes so any staff member can direct an individual to Health Information Management or the facility Privacy Officer.

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

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

Veterans are informed of the amendment process by many resources to include the Notice of Privacy Practice (NOPP) which states: Right to Request Amendment of Health Information. You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

1) File an appeal
2) File a "Statement of Disagreement"
3) Ask that your initial request for amendment accompany all future disclosures of the disputed health information. Information can also be obtained by contacting the facility ROI office.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

CDSP does not act as a definitive source of truth for data directly. It receives data from VA internal databases. Any redress requests should be directed to these VA sources.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

Consider the following FIPPs below to assist in providing a response:
<u>Principle of Individual Participation:</u> The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

<u>Principle of Individual Participation:</u> The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.
This question is related to privacy control IP-3, Redress.

Follow the format below:

<u>Privacy Risk:</u> Patients may not be aware of the processes for access, redress and correction.

<u>Mitigation:</u> The NOPP is provided to patients that contains all the information however if the patient did not receive it or does not remember, facility personnel are trained and should be able to direct the patient accordingly. The facility is responsible for quarterly monitoring that evaluates staff knowledge of the process, and any vulnerabilities are addressed with additional training and clarification.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

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

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

Veterans' Health Administration (VHA) has established policies and procedures for the identification and authorization of CPRS users. This application follows these previously established mechanisms. Access is restricted to VA employees who must complete both the Privacy and HIPAA Focused and Information Security training. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information Security Officer (ISO), local Chief Information Officer (CIO), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information. Users submit access requests based on need to know and job duties. Supervisor, ISO and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s)through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need-to-know basis.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Access requests are submitted for contractors and all outside agency requests and are processed through the appropriate approval processes. Users submit access requests based on need to know and job duties. Supervisor, Information System Owner (ISO) and Office of Information and Technology (OI&T) approval must be obtained prior to access granted. Once access is granted, individuals can log into the system(s)through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need-to-know basis.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Veterans' Health Administration (VHA) has established policies and procedures for the identification and authorization of CPRS users. This application follows these previously established mechanisms. Access is restricted to VA employees who must complete both the Privacy and HIPAA Focused and Information Security training. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information Security Officer (ISO), local Chief Information Officer (CIO), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information. Users submit access requests based on need to know and job duties. Supervisor, ISO and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s)through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need-to-know basis.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

Yes

8.2a. Will VA contractors have access to the system and the PII?

Yes

8.2b. What involvement will contractors have with the design and maintenance of the system?

VA contractors that have access to the computer system are only delegated keys and menu functions needed to complete their duty task. They are required to complete annual Privacy. Security, and Rules of Behavior training. Contractors having access to PHI/PII are required to have a Business Associate Agreement (BAA) (nationally with the Veterans Health Administration (VHA) or locally with facility). Contracts are reviewed on an annual basis by the Contracting Officer Representative (COR). The Privacy Officer and Information Security Officer monitor that the annual Privacy, Security, and Rules of Behavior (ROB) training is completed by contractors and business associates. Any local BAAs are monitored by Privacy Officer to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA). VA contractors under contract to perform system development and test system activities shall use redacted test patient data. No PII/PHI data is used in development or test systems. All contractors accessing VA systems or data are required to sign an NDA prior to beginning their work.

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

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

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

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

1. *The Security Plan Status:* Complete
2. *The System Security Plan Status Date:* 02-Oct-2024
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* Dec. 19th, 2023
5. *The Authorization Termination Date:* Dec. 18th, 2025
6. *The Risk Review Completion Date:* Oct. 10th, 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A; system is authorized.

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?
If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

The application resides on VAEC Amazon Web Services (AWS) as a Platform as a Service (PaaS) cloud model system.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). ***(Refer to question 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

The application resides on the VA Enterprise Cloud (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.

N/A, the application resides on the VA Enterprise Cloud (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.

N/A, the application resides on the VA Enterprise Cloud (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).

N/A, the application resides on the VA Enterprise Cloud (VAEC).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2025.04.03 15:01:38 -04'00'

Privacy Officer, Nancy Katz-Johnson

JENNIFER HUBA

Digitally signed by JENNIFER HUBA
Date: 2025.04.03 14:46:20 -04'00'

Information System Security Officer, Jennifer Huba

SHANE ELLIOTT

Digitally signed by SHANE ELLIOTT
Date: 2025.04.04 04:19:24 -07'00'

Information System Owner, Shane Elliott

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

SORN: 24VA10A7 (2020-21426.pdf [govinfo.gov])

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)