Privacy Impact Assessment for the VA IT System called:

Lung Cancer Screening Platform (LCSPv2)

Digital Service

Veteran's Health Administration (VHA)

Date PIA submitted for review:

October 28, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	nancy.katz-johnson@v.agov	203-535-7280
Information System Security Officer (ISSO)	Mike Yung	mike.yung@va.gov	215-823-5159
Information System Owner	Shane Elliot	shane.elliot@va.gov	909-435-1808

Abstract

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

This is a minor application associated w/the Clinical Decision Support Platform (CDSP) system hosted within the VA Enterprise Cloud (VAEC); Amazon Web Services (AWS). LCSPv2 is a Substitutable Medical Applications, Reusable Technologies (SMART) on Fast Healthcare Interoperability Resources (FHIR) based CDSP tool designed to assist clinicians and oncologists in the early detection of lung cancer in VA patients. It does so by working with an Enterprise Health Record (EHR) to pull in patient data and correlate clinical codes associated with their use of tobacco and associated health conditions in order to identify the patient's risk for developing lung cancer. LCSPV2 resides within the CDSP AWS cloud with the exception of pulling data from and performing analytics on the VA Rockies platform. As a SMART on FHIR application, it will be available for launch by VA sites on an opt-in basis similar to COVID-19 Patient Manager (CPM) through Computerized Patient Record System (CPRS) and, eventually, CERNER. LCSPv2 builds upon the version 1 model to create an electronic health record (EHR)-agnostic tool that works with both legacy (CPRS/VistA) and Cerner, enabling sites to use LCSPv2 regardless of EHR.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Lung Cancer Screening Platform (LCSPv2) is owned and operated by Digital Service under the Veteran's Heath Administration (VHA).

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

The business purpose is as follows: LCSPv2 addresses Customer Service and Transforming Business Operations. This will help clinicians to administer a high standard of care by adhering to new clinical guidelines. It will also help clinicians to work more efficiently by assisting with managing and acting upon the high volumes of data clinicians must work with, including rapidly evolving inpatient data, outpatient symptoms monitoring, and other patient-generated data. This clinical decision support application will provide recommendations at the point of care, overcoming current shortfalls to integrate them into the electronic health record (the centerpiece of clinician workflow).

C. Indicate the ownership or control of the IT system or project.

Lung Cancer Screening Platform (LCSPv2) is owned and operated by Digital Service under the Veteran's Heath Administration (VHA).

2. Information Collection and Sharing

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

Clinicians will store the data for veteran's and dependents on the application. There will be an estimated total of 1000 users of the application which the data will consist of full name, last 4 of ssn, age, problem list, diagnoses, vital signs, diagnostic tests, laboratory results, CT scans, and tobacco social history for veterans and dependents. There will also be an estimated total number of 3000 unique records on the system.

E. A general description of the information in the IT system and the purpose for collecting this information.

A general description of the information accessed by the system is as follows: LCSPv2 is a Substitutable Medical Applications, Reusable Technologies (SMART) on Fast Healthcare Interoperability Resources (FHIR) based CDSP tool designed to assist clinicians and oncologists in the early detection of lung cancer in VA patients. It does so by working with an Enterprise Health Record (EHR) to pull in patient data and correlate clinical codes associated with their use of tobacco and associated health conditions in order to identify the patient's risk for developing lung cancer. LCSPV2 resides within the CDSP AWS cloud with the exception of pulling data from and performing analytics on the VA Rockies platform. As a SMART on FHIR application, it will be available for launch by VA sites on an opt-in basis similar to Clinical Decision Support Platform (CDSP) through Computerized Patient Record System (CPRS) and, eventually, CERNER. LCSPv2 builds upon the version 1 model to create an electronic health record (EHR)-agnostic tool that works with both legacy (CPRS/VistA) and Cerner, enabling sites to use LCSPv2 regardless of EHR.

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

LCSPv2 does not share any data. The application is hosted on the internal VA network and all patient data is retrieved through Rockies. The application is a front-end application which does not send data back to other applications. 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 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 credential for the virtual box is stored in an Ansible vault file which is stored in a VA internal GitHub repository ("smart-on-fhir-inra"). It is encrypted using AES-256.

G. 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.

This system will be used in multiple VA Medical Centers. The same controls will be used across all sites. 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 SORN

H. A citation of the legal authority to operate the IT system.
The legal authority to operate this application is: SOR 24VA10A7 Patient Medical Records; Title 38, USC 501(b) and 304.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?
The current SORN does cover cloud usage and storage and does not need to be updated at this time the application operates in accordance with SOR 24VA10A7.

D. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes
The completion of this PIA will not result in circumstances that require changes to business processes.

K. Whether the completion of this PIA could potentially result in technology changes
The completion of this PIA will not result in technology changes.

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 Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Other Data Elements (list below)

Age, Problem List, Diagnoses, Vital Signs, Diagnostic Tests, Laboratory Results, CT Scans, Tobacco Social History

PII Mapping of Components (Servers/Database)

Lung Cancer Digital Platform consists of 1 key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Lung Cancer Digital Platform 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

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
LCS DB	Yes	Yes	Patient identifiers (full name, last 4 of ssn, age, problem list,	PII is restricted to internal use for storing information on qualified patients in sites that participate with	AWS Access Controls, DB credentials, security groups limiting access, encrypted

			diagnoses, vital signs, diagnostic tests, laboratory results, CT scans, tobacco social history	**the LCSPv2 program.**	**at rest, encrypted snapshots**

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

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

EHR (Cerner & VistA) is ingested into the corporate data warehouse (CDW) every day. Rockies (HDAP team) ingest the data into their data lake and the LCS team pulls that data from Rockies.

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.

This information is accessed from the electronic health record because the individual patient may not know the information. The system uses this information to make recommendations on next steps for care, which can be copy/pasted by a healthcare provide from the application into an electronic health record note if the provider would like to do that.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

EHR (Cerner & VistA) is ingested into the corporate data warehouse (CDW) every day. Rockies (HDAP team) ingest the data into their data lake and the LCS team pulls that data from Rockies.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

technologies or other technologies used in the storage or transmission of information in identifiable form?

EHR (Cerner & VistA) is ingested into the corporate data warehouse (CDW) every day. Rockies (HDAP team) ingest the data into their data lake and the LCS team pulls that data from Rockies.

1.3b 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.

N/A

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

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

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

Information is checked for accuracy within Rockies. Clinical practitioners review and sign all treatment information and Business Office/Health Information Management Service reviews data obtained and assists with corrections daily.

1.4b 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.

Clinical practitioners review and sign all treatment information and Business Office/Health Information Management Service reviews data obtained and assists with corrections daily.

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

24VA10A7/ 85 FR 62406 Patient Medical Records-VA 2020-21426.pdf (govinfo.gov)

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. (*Work with your System ISSO to complete this section)*

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

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

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

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

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

Follow the format below when entering your risk assessment:

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 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 system captures and stores information for qualified patients at participating LCSPv2 program sites. 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.

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

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

The system generates recommendations about a patient's care based on their clinical data. however, the recommendations are not stored or written back into the electronic health record.

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.

The system does not create or make available new or previously unutilized information about an individual, The system retrieves and displays data from VistA Rockies. 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 patient care.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

The 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.

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

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.

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

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.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

The system utilizes SSOi for authorization of users. Access to the system is restricted to authorized VA Medical Center personnel who already have access to the underlying data and are requesting access via LCSPv2.

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

The system utilizes SSOi for authorization of users. Procedures for access are documented in the Access Control policy. All users that require access to the system submits a SNOW access request ticket. This ticket is routed to the IAM team and they forward requests to a limited list of LCSPv2 administrators that approve all access request ensuring minimum level of access necessary to utilize the application in the performance of the users job. The approval queue is currently a manual process conducted by the LCSPv2 team. This process is documented in the LCSPv2 Coordinator Approval SOP.

2.4c Does access require manager approval?

The system utilizes SSOi for authorization of users. All users that require access to the system submits a SNOW access request ticket. This is currently a manual process targeting select sites and coordinators. Once requested, the ticket is routed to the IAM team and forwarded an IAM group

composed of a limited list of LCSPv2 administrators who approve all access requests. This ensures a minimum level of access necessary to utilize the application in the performance of the users job. While IAM has granted this role to members of the development team, eventually this role will be entrusted to another team as identified by project stakeholders.

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

The system utilizes SSOi for authorization of users. All users that require access to the system submits a SNOW access request ticket. This ticket is routed to the IAM team, and they forward requests to a limited list of LCSPv2 administrators that approve all access request ensuring minimum level of access necessary to utilize the application in the performance of the users job. IAM can provide access control lists upon request.

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

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*

The system does not retain data.

3.2 How long is information retained?

*In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods**. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

N/A – The system does not retain data.

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

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

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

N/A – The system does not retain data.

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

N/A – The system does not retain data.

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.

N/A – The system does not retain data.

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.

LCSPv2 does not use PII for research, testing, or training specifically that are mock accounts that are setup in the various toolsets.

3.6 <u>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 ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: N/A – The system does not retain data.

Mitigation: N/A – The system does not retain data.

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***
Rockies	To provide physicians with clinical data relevant to making decisions about patients.	Patient identifiers (full name, last 4 of ssn, age, problem list, diagnoses, vital signs, diagnostic tests, laboratory results, CT scans, tobacco social 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 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

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*
			("smart-on-fhir-infra"). It is encrypted using AES-256.

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

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

Follow the format below:

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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: N/A

Mitigation: N/A

Section 6. Notice

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

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

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

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

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. 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

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

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

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

The notice of privacy practices is a comprehensive document mailed to every eligible Veteran and available at every medical center and on line
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.

VHA permits individuals to agree to the collection and to the consent to the use of their personally identifiable information (PII) using paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. If the individual does not want their information collected or used, then they do not sign the consent form. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices (NOPP) and conversations with VHA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required. Where legally required VHA obtains signed, written authorizations from individuals prior to releasing, disclosing, or sharing PII and PHI. Individuals can request further limitations on other disclosures. The facility can approve or deny these requests. However, if the request to provide information is accepted the facility must conform to the restrictions

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

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

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

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

Privacy Risk: Since the Notice of Privacy Practices is sent via United States Postal Service, it's possible that a patient may not have received it.

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

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

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

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).

The system does not create any new patient information that the patient does not already have access to through the medical records system. All information that the system obtains is already

available in the patient's medical records (i.e. VistA, Cerner). The electronic medical record for VA has an established process for release of information to obtain a copy of or make changes to information the patient's electronic medical record.

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.

N/A –

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.

LCS does not collect 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 System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

Privacy Risk: Patients may not be aware of the processes for access, redress and correction

Mitigation: 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.

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

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.

8.1c 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 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.

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 anyVA 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 TMS system. 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
· VA PRIVACY & VA INFORMATION SECURITY

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

8.4a If yes, provide:

1. *The Security Plan Status:* Signed and Uploaded to eMASS, signed 12 Sep 22.
2. *The System Security Plan Status Date:* Signed and Uploaded to eMASS, signed 12 Sep 22.
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 12 Sep 22
5. *The Authorization Termination Date:* 12 Sep 23
6. *The Risk Review Completion Date:* 12 Sep 22
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 No or In Process, provide your ***Initial Operating Capability (IOC) date.***

ATO was granted on parent titled Clinical Decision Support Platform (CDSP), 30 Sep 21, and ATO was granted for 3 years, until 29 Sep 24. The minor application was approved as a minor under CDSP for a period of one year which start on 12 Sep 22 and expires 12 Sep 23, Categorization for the system is moderate.

Section 9 – Technology Usage

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

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

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

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

The application resides on the VA Enterprise Cloud (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). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

N/A

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

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

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

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

ID	Privacy Controls
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.

NANCY KATZ-JOHNSON

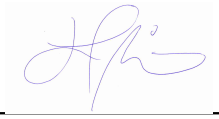
Digitally signed by NANCY KATZ-JOHNSON
Date: 2022.11.19 16:28:38 -05'00'

Privacy Officer, Nancy Katz-Johnson

Mike Yung 142156

Digitally signed by Mike Yung 142156
Date: 2022.11.21 14:37:43 -05'00'

Information Systems Security Officer, Mike Yung



Digitally signed by SHANE ELLIOTT
Date: 2022.11.21 11:01:59 -08'00'

Information Systems Owner, Shane Elliot

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).

The applicable SORN, 24VA10A7/85 FR 62406, 24VA is Patient Medical Records-VA located 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:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices