Privacy Impact Assessment for the VA IT System called:

Consult Toolbox (CTB)

Veterans Health Administration

Office of Integrated Veteran Care

Date PIA submitted for review:

01/18/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michael Hartmann	Michael.Hartmann@va.gov	303.780.4753
Information System Security Officer (ISSO)	Dewitt Sanders	Dewitt.Sanders@va.gov	818.891.7711.ext 36281
Information System Owner	Temperance Leister	Temperance.Leister@va.gov	484.432.6161

Abstract

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

Consult Toolbox (CTB) standardizes the documentation process and workflow of VA staff (clinical and administrative) managing referrals for internal care and community care. In conjunction, CTB works within two components The Decision Support Tool (DST) and The Decision Support Viewer (DSV). DST enables VA care providers to determine whether a given Veteran is eligible for and would be best served by utilizing the Veterans Community Care Program, in real-time, with the Veteran in the exam room. It then documents the decision rationale in the Veteran's health record and is integrated into the existing Computerized Patient Record System (CPRS) consult order workflow. DST allows the care provider on the VA network to login to a web interface using their VA Personal Identity Verification (PIV), with a Veteran/Patient present, to view relevant data within the existing CPRS consult order workflow. This tool helps the Veteran and VA provider to decide if a consult service should be referred to the local VA facility, a near-by VA facility via an Inter-Facility Consult (IFC), or to a community provider streamlining the VA acceptance and storage of medical PDF records received from community providers and stores them in the Veterans Health Information Systems.

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.

Consult Toolbox is sponsored by Enterprise Program Management Office (EPMO), Telehealth and Community Care product line. The Consult Toolbox (CTB) is a web application that is invoked during the consult management workflow in Computerize Patient Record System (CPRS).

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

CTB utilizes various microservice components to support consult management activities by VA administrative and clinical staff on the VA network. CTB is used to simplify the process of consult management. During the life of a consult there are prescribed steps of actions taken and CTB fulfills a need to track these steps at an individual patient level by recording consistent responses in the Veteran's VistA electronic health record (EHR). CTB uses a web interface to allow staff, on the VA network with a valid PIV, to document consult actions quickly and consistently. It uses consistent verbiage to document consult steps and eliminates the need to take a second action or make a separate entry to track scheduling steps. The overall CTB system provides a consistent user experience, minimizes the reduce costs associated with development and sustainment activities, and enhances the overall security posture of the system. Additionally, it provides an understanding of the overall status of consult management at a macro level and highlights specific services needing attention or resources.

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

CTB is VA Owned and Operated.

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.

The system is accessed by clinicians at treatment facilities across the VA network the number of records in the system could be up to 3,000,000. The clinician can log into the system at their workstation and review the Veteran's consult results with the Veteran present.

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

CTB captures data and documentation from internal sources that helps the Veteran and VA provider to decide if a consult service should be referred to the local VA facility, a near-by VA facility via Inter-Facility Consults (IFC), or to a community provider by providing information about the drive time standards associated with the Standardized Episodes of Care (SEOC) related to requested consult service, average wait times and quality metrics for in-house/IFC consults within the drive time standards of the Veteran's place of residence, and Veteran's eligibility for accessing care in the community and their stated preferences (opt-in/out). Several systems are used to assist in providing this information. This includes Corporate Data Warehouse (CDW) that provides treatment facility information, Enrollment System Redesign that provides patient eligibility information, Lighthouse API provides facility location and drivetime information, Community Care Referrals and Authorizations (CCRA) provides referral status information, Standardized Episodes of Care (SEOC) provides episodes of care information, Computerized Patient Record System (CPRS) provides episodes of care information, VISTA that stores all CTB decision data after consult signature, and SSOi is used to authenticate users.

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

Information is stored and can be accessed by interconnected Veteran Health Systems as required to provide care.

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.

The CTB system is located in the VAEC Cloud.

3. Legal Authority and SORN

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

23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015)
24VA10A7, Patient Medical Records - VA (10-2-2020)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015)
58VA21, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records -

VA (8-11-2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) - VA (12-23-2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8-13-2018)
89VA10NB, Income Verification Records - VA (12-19-2013)
97VA10, Consolidated Data Information System - VA (12-23-2020)
114VA10, The Revenue Program-Billing and Collections Records - VA (1-25-2021)
121VA10P2, National Patient Databases - VA (2-12-2018)
147VA10, Enrollment and Eligibility Records - VA (8-17-2021)
155VA10NB, Customer Relationship Management System (CRMS) - VA (3-3-2015)
172VA10, VHA Corporate Data Warehouse - VA (12-22-2021)

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?

SORNs do not need revision for approval.

D. System Changes

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

This PIA will not require changes in business processes. This PIA will not result in technology changes. A SORN does not apply to the CTB Project, no changes to existing SORNS are required. The system will utilize the VAEC AWS Cloud environment. The CTB is not a Software as a Service (SaaS) product. This deployment utilizes the VAEC AWS Cloud as a Platform as a Service (PaaS) deployment. The system is expected to complete the VA's Risk Management Framework (RMF) process and obtain an Authority to Operate (ATO) through Veterans Affairs (VA).

K. Whether the completion of this PIA could potentially result in technology changes

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)

Zip Code
GEO Coordinates
Consult Factors
Consult History

Community Care Consult Name
Consult Type
Urgent Care Eligible
Community Care Eligibilities
Veteran Choice Eligibility Codes
Clinical Service
Urgency
Clinically Indicated Date (CID)/No Earlier Than Date
No Later Than Date
Event Risk Date,
Execute Date
Insert Date
Drive Time Standard
Wait Time Standard
Standard Episode of Care (SEOC) w/ Description
Consult Stop Code Description
Facility Name
Average Wait Time
Drive Time
Best Medical Interest of Veteran Justification
VA UserID

PII Mapping of Components (Servers/Database)

CTB consists of one 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 CTB and the reasons for the collection of the PII are in the table below.

The CTB system uses AWS PostgreSQL database to temporarily store the results of data collection for up to 30 days. Multiple Application Program Interfaces (APIs) and webservices are used to make calls to 6 data sources.

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
CTB Database	Yes	Yes	Name, Date of Birth, Integration Control Number (ICN), Consult History, Community Care Eligibilities, Consult Factors, Community Care Consult Name, VA User ID, Best Medical Interest of Veteran Justification	CTB Data is stored as a local copy of decision information to speed retrieval of the patient data	Secure Socket Layer/Transport Layer Security (SSL/TLS) Connections, Data is encrypted at rest

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?

The CTB system collects the data from other internal VA systems to automate the information retrieval and to present the data to the clinician and Veteran in a way that helps the Veteran understand choices for treatment. The CTB system does not use commercial data aggregators.

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.

The CTB system collects the data from other internal VA systems to automate the information retrieval and to present the data to the clinician and Veteran in a way that helps the Veteran understand choices for treatment. No commercial aggregator is used for CTB.

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

The CTB system does not create new information. It retrieves information from other internal VA systems.

1.3 How is the information collected?

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

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

Information maintained in CTB is originated in other VA systems. The information is gathered at the point of service (care in the VA Medical Center).

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.

No information for CTB is directly collected manually on a form. All data is automatically retrieved from other information systems during the Computerized Patient Record Service (CPRS) standard consult workflow, as detailed in section 4.1 below. Within the CPRS order consult workflow, care providers will utilize the CTB system to support the decision and election for consult services for a given consult with the patient.

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.

The CTB system includes error handling processes in the workflow. If errors are encountered the system will prompt the user check the displayed data. CTB data is displayed in the application and the clinician and Veteran will, in the course of the patient consult, review all information and have the opportunity to verify and if necessary, update the collected information. Details on updating information are contained in section 7.2 below

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.

CTB does not use a commercial aggregator for accuracy system checks.

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

- VACAA (Public Law 113–146)
- Amendment to VACAA (Public Law 115-26)
- HIPAA (Public Law 104-191)
- 45 CFR 164.506 Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations
- 38 USC 8111 and 10 USC 1104
- 25 USC Sections 1645, 1647
- 38 USC Sections 523(a), 6301-6307
- 38 USC 815
- 32 CFR 806b.12 - Requesting the Social Security Number

Systems of Records Notices:
23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015)
24VA10A7, Patient Medical Records - VA (10-2-2020)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3/-015)
58VA21, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (8-11-2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) - VA (12-23-2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8-13-2018)
89VA10NB, Income Verification Records - VA (12-19-2013)
97VA10, Consolidated Data Information System - VA (12-23-2020)
114VA10, The Revenue Program-Billing and Collections Records - VA (1-25-2021)
121VA10P2, National Patient Databases - VA (2-12-2018)
147VA10, Enrollment and Eligibility Records - VA (8-17-2021)
155VA10NB, Customer Relationship Management System (CRMS) - VA (3-3-2015)
172VA10, VHA Corporate Data Warehouse - VA (12-22-2021)

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*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: Unauthorized access by VA employees to the Consult Toolbox and the information the system contains.

Mitigation: Access to the system is granted by local administrators to eligible health care providers that need to access a patient's medical records. Security control AC-06 and enhancements governing least privilege are in place to mitigate the risk. Users of the system are required to take Talent Management System (TMS) training pertinent to their general role at the VA. This includes understanding HIPAA and rules of behavior. Additionally, the following technical controls have been implemented to ensure data is limited to those individuals with a need to know and who already have access to patient data via the Electronic Health Record Modernization (EHRM) system used to access the system

- Access to records is limited to the user who created the record or users who are accessing records through authorized client applications
- Access to records, even for the originating user are locked after 5 minutes unless being accessed via authorized client applications
- All records are deleted from the system following 30 days of inactivity

Privacy Risk: Personally Identifiable Information (PII) of a Veteran/Beneficiary may not be accurate, complete, and current in system.

Mitigation: CTB relies on the source (feeder) systems to ensure that personally identifiable

information is accurate, complete, and current. The following policies and procedures in the VA ensure that any PII collected and maintained by VA is accurate, relevant, timely, and complete for the purpose for which it is to be used:

- Requires a Veteran or an authorized representative to validate PII during the collection process
- When required, requests Veteran or an authorized representative to revalidate that PII collected is still accurate
- Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;
- Collects PII directly from the individual to the greatest extent practicable
- Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems; and
- Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

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 Consult Toolbox (CTB) system will be used to enable VA care providers to determine whether a given Veteran is eligible for and would be best served by utilizing the Veterans Community Care Program, in real-time, with the Veteran in the exam room. It then documents the decision rationale in the Veteran's health record and is integrated into the existing CPRS consult order workflow.

This helps the Veteran and VA provider to decide if a consult service should be referred to the local VA facility, a nearby VA facility via Inter-Facility Consults (IFC), or to a community provider.

All data collected is necessary to support the function of the application. The Veteran Name, DOB, are collected to uniquely identify the patient. Residential Address is collected to determine distance and drive time to treatment facilities. The ICN is collected to determine eligibility. Computerized Patient Record System (CPRS) data is used to determine the patient's condition and personal information; Enrollment system information is used to determine the patient's eligibility to receive care; Lighthouse API information shows provider facilities and distance from the patient's home; Standardized Episode of Care (SEOC) information is the description of the care to be received; Corporate Data Warehouse (CDW) shows if the facility can provide care and wait times.

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.

CTB retrieves all data from other existing internal systems. Data is received over secure communication channels and when ingested, the data is run through validation filters remove any malicious information. CTB is live access system, where the data is called by the clinician on a case-by-case basis. The clinician will determine if the information is valid for the given patient. If corrupt or incomplete data is encountered, an error message will be displayed to the clinician.

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.

CTB will provide the following types of information for the clinician and Veteran:

- Veteran's eligibility for accessing care in the community and their stated preferences (opt-in/out)
- Average wait times and quality metrics for in-house / Inter-Facility Consults (IFC) consults within the drive time standards of the Veteran's place of residence
- Drive time standards associated with the SEOC related to the requested consult service.
- Allows the provider to select the referral decision and enter additional justification text when indicated.
- Generates structured text based on the displayed results that can be used for downstream report generation.
- Provide required information to the Electronic Medical Record (EMR) to initiate either an in-house, IFC, or Veteran Community Care Program (VCCP) consult order, based on the decision outcome.
- Documents the rational for the referral decision and other consult actions in the consult record.

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?

Data is encrypted in transit using TLS/SSL encryption and is encrypted at rest.

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

N/A

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

See item 2.3a

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to CTB is granted on a need-to-know basis at the treatment facility. VA staff must complete an access request through a Service Now (SNOW) ticket, which must be signed by staff (requester) and employee's supervisor approval. The local Office of Information Technology (OIT) will verify staff completed Privacy, Cyber Security Training, and Signed Rules of Behavior in TMS by signing the Access Request Form. This form will be sent to a designated mail group as evidence of compliance and authorization to use the system. The OIT will sign the Access Request Form, only at this point will access be granted by the application administrators.

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

Access to CTB is first based on user access to the CPRS system. VA staff (clinicians) use a Personal Identity Verification, (PIV), to access their workstation creating an initial authorization to gain access to the VA network. The clinician then signs into the CPRS. For authentication, CPRS utilizes a

Veterans Health Information Systems and Technology Architecture (VistA) user identification number and PIN for access, and it holds its own user tables and authorization list.

2.4c Does access require manager approval?

CTB does not require a manager's approval for access.

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

When the CTB application is called, users will authenticate using Single Sign On internal (SSOi). System access and activity is logged and recorded. VA Clearance procedures are implemented to monitor access, and accounts are disabled after 30 days of inactivity.

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

VHA ensures that the practices stated in the PIA are reinforced by requiring Contractors and VA employees to complete all VA trainings including VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203). Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply. Through TMS employees and contractors are monitored, CORS are responsible for ensuring assignment in TMS training. Training audits occur monthly and are conducted by ISSOs throughout the VA. Training records are stored in the TMS system. Any user who is not current in Privacy/Infosec training loses access to all VA data (including DAPER) until they become current on required training. All incidents are required to be reported to the supervisor or ISSO / Privacy Officer within 1 hour of occurrence. If the ISSO determines a security event has occurred, they open a PSETS ticket and inform CSOC and DBRS. Credit monitoring may be provided to any person whose sensitive information has been violated, and the system user who put the data at risk will be retrained and consequences of actions up to loss of job.

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*

Patient name (First, Last, Middle), Consult Service, Date of Birth, Mailing Address, Telephone Number

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.*

The CTB Database is considered temporary storage of the specific consult information. All information stored in the temporary CTB database will be deleted 30 days after consult is signed or 30 days after an un-signed session is stored and not signed. A python script will execute nightly to query records with a last modified date greater than 30 days from the PostgreSQL database. The records returned from that query will be permanently deleted. Persistent CTB documentation is written and maintained outside of the CTB boundary in CPRS (consult record comments) and CDW (analytics reporting table).

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. 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?

CTB is not a system of record. Data is compiled from other sources and results are sent to VistA to be retained. Interim electronic source information is compiled, as noted in 6600.2, and the information is destroyed after migration to the electronic health.

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

6000.2 Electronic Health Record (EHR). CTB follows the VHA Records Control Schedule (RCS 10-1) located at https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

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.

The CTB database will be deleted after decommissioning, following the Records Control Schedule (RCS 10-1), in compliance with VA policy, by physically deleting the stored data then overwriting the drives with generic/dummy data to ensure no previous ghost/residual data can be restored. Paper destruction in N/A because there are no paper records.

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.

Data in this system is not used for research, testing, or training.

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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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.

<u>Privacy Risk:</u> The risk that Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) may be breached increases the longer the information is retained.

Mitigation: To combat the risk of PII and other Sensitive Personal Information being breached the CTB system incorporates encryption and secure data transfer protocols and features. Unnecessary records are purged.

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***
Computerized Patient Record System (CPRS)	CPRS Data is used to determine the patient's condition	Consult Service, Clinically Indicated Date (CID)/No	Application Programming Interface (API),

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
	and personal information	Earlier Than Date, Urgency, Name, Date of Birth (DOB)	Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Connections
Enrollment/Eligibility (E&E/ESR) Service	Enrollment & Eligibility system information is used to determine the patient's eligibility to receive care	Address, Zip Code, Veteran Choice Eligibility Code, GEO Coordinates, Phone Number	API, SSL/TLS Connections
Standardized Episode of Care (SEOC)	SEOC information is the description of the care to be received	Standard Episodes of Care (SEOC), Consult Type	API, SSL/TLS Connections
Corporate Data Warehouse (CDW)	CDW Information shows if the facility can provide care and wait times	Consult Type, Consult Stop Code Description, VA UserID, Community Care consult Name, Average Wait Time	Data adapter, SSL/TLS Connections
Corporate Data Warehouse (CDW)	CDW Information for the CANScore	Integration Control Number (ICN), Event Risk Date, Execute Date, Insert Date	API, SSL/TLS Connections
Veterans Health Information System Technology Architecture (VistA)	The Veteran record in VistA is updated with non-PII data that is displayed in the CTB page, such as the facility info, date of service, drive time to facility, consult type	Name, Date of Birth, VA User ID, Integration Control Number (ICN), Consult History, Community Care Eligibilities, Consult Factors, Consult Type, Veteran choice eligibility Codes	Data adapter, SSL/TLS Connections
Lighthouse	Lighthouse is a VA API used to retrieve provider facilities and distance from the patient's home	GEO Coordinates.	SSL/TLS/REST
SSOi	SSOi is used to authenticate and authorize users	VA UserID	SSL/TLS Used as authentication

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.

Privacy Risk: There is a risk that information may be accessed by an unauthorized VA employee or persons without a need to know.

Mitigation: System is only available to authorized VA employees. SSOi validates user's account against PIV/Windows Active Directory authentication. All access is monitored, tracked, and logged.

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.

The CTB data is retrieved from other VA systems. No new data is collected from individuals.

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

Privacy notices are provided at the point of service at the medical center where the Veteran receives care, in accordance with VHA Handbook 1605.4, Notice of Privacy Practices. Notice of privacy practices are available at https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946v. Each of the above notices includes information on how to report any use of information that is not in accordance with the collection.

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.

Privacy notices are provided at the point of service at the medical center where the Veteran receives care, in accordance with VHA Handbook 1605.4, Notice of Privacy Practices. Notice of privacy practices are available at https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946. Each of the above notices includes information on how to report any use of information that is not in accordance with the collection.

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

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

VHA Directive 1605.01 "Privacy and Release Information" lists the rights of beneficiaries to request the VHA to restrict the use and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. Veterans and their Beneficiaries have the right to refuse to disclose their SSNs to the VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (please refer to the 38 Code of Federal Regulations CFR 1.575(a)).

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 Directive 1605.01, "Privacy and Release Information" list the rights of Veterans and their Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: Has sufficient notice been provided to the individual?

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

Privacy Risk: If notice is not provided in a timely manner, an individual may give information that they do not want to be shared.

Mitigation: Privacy practice notices are provided to the Veteran at the time of service. This is in accordance with (IAW) VHA Handbook 1605.04 NOTICE OF PRIVACY PRACTICES.

Section 7. Access, Redress, and Correction

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

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

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

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

VHA Directive 1605.01: Privacy and Release Information states the rights of Beneficiaries to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement.

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).

All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office.

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.

All requests for access to data must be delivered to, and reviewed by, the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Any corrections to a Veteran's data would be done at the source systems. In the event that data stored in the authoritative sources are erroneous, the CTB personnel can take a note, but cannot correct inaccurate or erroneous information. However, if a correction is requested by a Veteran or Provider, then such a request must be in writing and it must adequately describe the specific information that the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. VHA Directive 1605.01, Appendix D: "Privacy and Release Information", Section 5 lists the rights of Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations.

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

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

A notice of privacy practices is provided at all VA Medical Centers, which includes the following: Individuals have a right to contact the VHA call center to gain access to their information. Right to Request Receipt of Communications in a Confidential Manner. Right to request that the VA provides the Veterans and their beneficiaries' health information by alternative means or at an alternative location. VA will accommodate reasonable requests, as determined by VA/VHA policy, to receive communications containing the beneficiaries' health information at a mailing address (e.g., confidential communications address) other than the beneficiaries' permanent address, or in person under certain circumstances.

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

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

If a Veteran discovers that incorrect information was provided during the intake process, the request to change the information must be in writing and adequately describe the specific information the Veteran believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager,

or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Privacy Risk: There is a risk that a Veteran could accidentally provide incorrect information to the VA, and that data could make its way into CTB.

Mitigation: A Veteran who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or who wants to review the contents of such a record, should submit a written request or apply in person to the VA health care facility (or directly to the VHA) where care was rendered. Inquiries should include the patient's full name, SSN, and return address.

Section 8. Technical Access and Security

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

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

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.

Access to the CTB system is limited to CPRS users

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?

VA staff who have taken the required training and agreed to rule of behavior will have view only access 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.

All users must be VA cleared.

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.

Only authorized development contractors will have direct access to the CTB database. The Office of Integrated Veteran Care (IVC) is responsible for ensuring that all contractors who are working on IVC projects have signed Non-Disclosure Agreements and met any necessary contractual requirements governing access and handling of Veteran data. All personnel will be required to complete all necessary on-boarding information, paperwork, and training. Before contractors onboard to the CTB project team, OCC leadership is required to ensure that all contractors interfacing with CTB project team and CTB data are adhering to VA policies and OMB Memorandum M-06-15 and OMB Memorandum M-06-16. According to OMB Memorandum M-17-15, OMB Memorandum M-06-16 is rescinded and captured within other policies and NIST standards (https://policy.cio.gov/rescissions-identity-management).

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

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

Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's Talent Management System (TMS). After the personnel's initial acceptance of the Rules, they must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training.

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

VA 3195: Information Security for CIOs Executives, Senior Managers, CIOs and CFOs
VA 3197: Information Security Role-Based Training for IT Specialists
VA 10176: Privacy and Info Security Awareness and Rules of Behavior
VA 10203: Privacy and HIPAA Training
VA 64899: Information Security Role-Based Training for IT Project Managers
VA 3812493: Annual Government Ethics Role-based Training
VA 1357076: Information Security Role-Based Training for System Administrators
VA 1357083: Information Security Role-Based Training for Network Administrators
VA 1357084: Information Security Role-Based Training for Data Managers
VA 3867207: Information Security Role-Based Training for System Owners

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 27- Jul- 2021
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* 03-Dec-2020
5. *The Authorization Termination Date:* 03-Dec-2023
6. *The Risk Review Completion Date:* 23-Nov-2020
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.***

N/A

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)*

CTB system utilizes 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
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

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

Signature of Responsible Officials

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

Michael D Hartmann 1612370

Digitally signed by Michael D Hartmann 1612370
Date: 2023.04.03 11:10:42 -06'00'

Privacy Officer, Michael Hartmann

DEWITT SANDERS

Digitally signed by DEWITT SANDERS
Date: 2023.04.05 07:10:48 -07'00'

Information Systems Security Officer, Dewitt Sanders

Temperance M. Leister 3514567

Digitally signed by Temperance M. Leister 3514567
Date: 2023.04.05 09:47:12 -06'00'

Information Systems Owner, Temperance Leister

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).

- Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES
- **23VA10NB3,** Non-VA Care (Fee) Records - VA (7-30-2015)
- **24VA10A7,** Patient Medical Records - VA (10-2-2020)
- **54VA10NB3,** Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015)
- **58VA21,** Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (8-11-2021)
- **79VA10,** Veterans Health Information Systems and Technology Architecture (VistA) - VA (12-23-2020)
- **88VA244,** Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8-13-2018)
- **89VA10NB,** Income Verification Records - VA (12-19-2013)
- **97VA10,** Consolidated Data Information System - VA (12-23-2020)
- **114VA10,** The Revenue Program-Billing and Collections Records - VA (1-25-2021)
- **121VA10A7,** National Patient Databases - VA (2-12-2018)
- **147VA10,** Enrollment and Eligibility Records - VA (8-17-2021)
- **155VA10NB,** Customer Relationship Management System (CRMS) - VA (3-3-2015)
- **172VA10,** VHA Corporate Data Warehouse - VA (12-22-2021)

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